HAND BOOK ON CURRENT CYBER CRIMES

A Simple Guide to Know about Cyber Crimes



JOINT INITIATIVE OF VIZAG CITY POLICE
&
VIZAG SECURITY COUNCIL

VISAKHAPATNAM CITY SECURITY COUNCIL (VCSC)

Visakhapatnam City Security Council (VCSC) is a not-for-profit initiative and a collaboration between Visakhapatnam City Police and Manufacturing industries, Service Industries and IT industry. Visakhapatnam city police launched VCSC, along with the Captains of Industry in Visakhapatnam to increase the preparedness pertaining to safety and security of businesses and citizens.

OUR EXECUTIVE COUNCIL



Dr. A. Ravi Shankar, IPS

Honorary Chairman



A.K.Balaji

Secretary



Lakshmi Mukkavalli

Joint Secretary (Women)



R.L.Narayana

Joint Secretary (Projects)



Dheeraj

Treasurer



Sreedhar Kosaraju

Advisor

ముందుమాట



ఈ డిజిటల్ ప్రపంచంలో, సాంకేతికత మనిషి జీవితంలో ప్రతి అంశంలో విస్తరించి ఉన్నది. సైబర్ క్రైమ్ ముప్పు గతంలో కంటే ప్రస్తుతం ఎక్కువగా ఉన్నది ఇంటర్నెట్ అందించే సౌలభ్యాలు మరియు అవకాశాలను స్వీకరించినపుడు ప్రతిఫలంగా ప్రపంచ వ్యాప్తంగా సమాజాన్ని ప్రభావితం చేసి, లాభాలా కోసం దుర్బలత్యాలని ఉపయోగించికోవాలని హానికరమైన నటులు, వ్యక్తులు, వ్యాపారాలు నుండి ఎదురయ్యే స్వాభావిక నష్టాలను కూడా మనం ఎదుర్కోవాల్సి ఉంటుంది.

" A simple guide to know about cyber crime" అను పుస్తకం, ప్రస్తుతం జరుగుతున్న సైబర్ నేరాలను వివరిస్తూ పెరుగుతున్న సైబర్ బెదిరింపులను ఎదుర్కొవడానికి మరియు సైబర్ నేరాల నుండి మనల్ని మనం రక్షించుకోవడానియిక ఒక ప్రత్యేకమైన వనరుగా పనిచేస్తుంది. ప్రస్తుం మనం గమనిస్తున్న కేస్ స్టడీస్ మరియు అభివృద్ధి చెందుతున్న సైబర్ మోసాలను నిరోధించడానకి మరియు ప్రతి స్పందించడానికి అవసరమైన జ్ఞానం మరియు అవగాహనతో పాఠకులను ఇది సన్నద్ధం చేస్తుంది.

బాధితులపై తక్షణ అర్థిక మరియు భావోద్వేగ నష్టానికి మించి, సైబర్ క్రైమ్ అనేది మన యొక్క సామూహిక భద్రత అర్థిక స్థిరత్వం మరియు సామాజక శ్రేయుస్సుకు ముప్పును కటిగిస్తుంది.క్లిష్టమైన అవస్థాపనను లక్ష్యంగా చేసుకునే దాడుల నుండి మానవ మానస్తత్వ శాస్త్రాన్ని దోపిడీ చేసే సామాజిక ఇంజనీరింగే పథకాల వరకు సైబర్ నేరగాళ్ళు ఉపయోగించే వ్యూహాలు అధునాతనత స్థాయిలో అభివృద్ధి చెందుతూనే ఉన్నాయి.

నేషనల్ సైబర్ క్రైమ్ రిపోర్టింగ్ పోర్టల్, NCRP 1930, CFCFCRMS లో నివేదించబడిన వివిధ రకాల సైబర్ మోసాలు క్రింద విశాఖపట్న్న నగరంలో ఉప్పటి వరకు 12,000 బాధితులు మోసపోయారు. అందులో సుమారుగా 85,51,90,001 రూ నష్టపోగా అందులో 8,90,29,320 హోల్డ్‌లో ఉంచబడినది.

అవగాహన అనేది సైబర్ నేరాలకు వ్యతిరేకంగా రక్షణలో మొదట వరస సైబర్ నేరాగాళ్ళు ఉపయోగించే వ్యూహాలను అర్థం చేసుకోవటం ద్వారా మరియు తాజా సైబర్ సెక్యూరిటీ బేస్డ్ ప్రాక్టీస్ గురించి తెలియజేయడం ద్వారా వ్యక్తులు మరియు సంస్థలు తమ యొక్క ఎక్స్‌పోజర్‌ను తగ్గించుకొని, డిజిటల్ ఆస్థులను కాపాడుకోవచ్చు.

వైజాగ్ సిటీ పోలీస్ మరియు విశాఖపట్నం సెక్యూరిటి కౌన్సిల్ యొక్క ప్రయత్నాలు సైబర్ బెదిరింపుల ద్వారా ఎదురైె సవాల్లును ఎదుర్కోవటంలో విద్య, అప్రమత్తత మరియు సహకారం యొక్క ప్రాముఖ్యతను నొక్కి చెబుతున్నాయి.

నమ్మకం సమగ్రత మరియు ఆవిష్కరణలు వృద్ధి చెందడం ద్వారా సాంకేతికత యొక్క ప్రయోజానాలు అందరూ ఆస్వాదించడం ద్వారా మనం మరింత సురక్షితమైన మరియు స్థితిస్థాపకమైన సైబర్ పర్యావరణ వ్యవస్థను నిర్మించగలము.

డా॥ ఎ. రవిశంకర్, ఐపియస్.,
కమీషనర్ ఆఫ్ పోలీస్ &
అదనపు జిల్లా మెజిస్ట్రేట్
విశాఖపట్నం మెట్రో పాలిటన్ సిటీ, ఆంధ్రప్రదేశ్

విషయసూచిక

స్టాక్ ఎక్స్ఛేంజ్ / ట్రేడింగ్ ఇన్వెస్ట్‌మెంట్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి తస్మాత్ జాగ్రత్త... స్టాక్ ఎక్స్చేంజ్/ ట్రేడింగ్ ఇన్వెస్ట్‌మెంట్ పేరుతో ఫ్రాడ్ చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు..., సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్‌లకి సవాలు విసురుతున్నారు. వాట్సప్, టెలిగ్రామ్ లేదా ఇతర సోషల్ మీడియా ప్లాట్‌ఫామ్ లో మనలని జాయిన్ చేసి లాభాలు వస్తాయి అని చెప్పి వివిద రకాల స్టాక్సు కొనడానికి అని చెప్పి వారి చెప్పిన అకౌంట్స్‌లో డబ్బులు వేయించుకొని మోసం చేస్తున్నారు, మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనార్హం..., సైబర్ క్రైమ్ పోలిస్ స్టేషన్‌లో విపరీతంగా క్రైమ్ రేట్ పెరుగుతుంది. కారణం, చదువుకున్నవారు ముఖ్యంగా సాఫ్ట్‌వేర్ ఉద్యోగులు, ట్రేడింగ్ చేసేవారు, గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

నేర విధానం వివరంగా :

1. మొదటిగా సైబర్ నేరగాళ్ళు నేరం చేయటానికి సోషల్ మీడియా ప్లాట్‌ఫామ్ అయినటువంటి వాట్సాప్, టెలిగ్రామ్, ఫేస్‌బుక్, ఇన్స్టాగ్రామ్ నందు గ్రూప్స్ క్రియేట్ చేసి అందులో ఎవరైతే ట్రేడింగ్ చేస్తారో బ్రోకరేజ్ అప్లికేషన్ అయిన ఏంజిల్ బ్రోకింగ్, Growup, Sharekhar, Zeroda మరియు వివిద రకాల వాటిలోనే ఫోన్ నెంబర్స్ మరియు ఇతర డాటాని సంపాదించి గ్రూప్‌లో యాడ్ చేస్తారు.
2. ఎవరైతే ఆ గ్రూప్‌లో జరుగుతునవని గమనించి నిజంగానే స్టాక్‌లో లాభాలు వస్తున్నాయి అని నమ్మి రెస్పాండ్ అవుతారో వారికి లాభాలు ఆశ చూపిస్తూ స్టాక్‌ను కొనే లేదా అమ్మే విధంగా విధంగా ఫేక్ వెబ్‌సైట్స్ డిజైన్ చేయబడుతుంది.

3. బాధితుడుకి వాట్సాప్‌లో తెలియకుండ ఒక గ్రూప్‌లో యాడ్ అవుతాడు తరువాత అందులో ఆ గ్రూప్ పేరు స్టాకు పెట్టుబడి సలహాలు అని వుంటుంది మరియు ఆ గ్రూప్‌లో చాలా మంది సభ్యులు ఉంటారు.

4. మొదటిగా అందులో స్టాక్ ఎక్కడెక్కడ కొనాలి లేదా అమ్మాలి అనే సలహాలు ఇస్తారు. ముఖ్యంగా ఇండియాలో స్టాక్ ఎక్స్చేంజ్‌లో ట్రేడింగ్ చేసి తరువాత ఆ స్టాక్ LU (Lower Circuit), UP (Upper Circuit) లో ఉండడం వల్ల మనం కొనలేని లేక అమ్మలేని పరిస్థితిలో అనే కాన్సెప్ట్‌తో Fraudster వస్తాడు.

5. ఎవరైతే ఆ గ్రూప్‌లో జరుగుతునవని గమనించి నిజంగానే స్టాక్‌లో లాభాలు వస్తున్నాయి అని నమ్మి రెస్పాండ్ అవుతారో వాళ్ళకి మొదటిగా ఫారన్‌లో డి-మార్ట్ అకౌంట్ ఓపెన్ చేయాలి అని చెపుతారు అదే విధంగా కొన్ని అకౌంట్స్‌ని చూపిస్తారు.

6. ఇండియాలో స్టాక్ కొనలి అంటే అమైంట్ డాలర్ రూపంలో ఉండాలి కాబట్టి మీరు మేము పంపిన అకౌంట్‌లో డబ్బులు వేయండి అని డాలర్‌లో మార్చి ఇండియాలో స్టాక్స్ కొనవచ్చు అని చెపుతారు.

7. అప్పుడు బాధితుడుకి వాళ్ళు ఇచ్చిన అకౌంటులోకి డబ్బులు పంపి IPO(Initial Public Offering) డిటైల్స్ ఉంటాయి అని చెపుతారు.

8. మనం ఆ Proxy Website లో చూడగా అందులో అంతా చాలా చెన్యూన్‌గా ఉంటుంది కానీ అది నిజం కాదు. మనకి ఎటువంటి ఫండ్స్ రావు మరియు డబ్బులు వేసి మోసపోతాం.

9. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళు చేతిలో తాను నమ్మినంత వరకు డబ్బులు వేసి మోసపోతారు.



క్రిప్టో కరెన్సీ ట్రేడింగ్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి తస్మాత్ జాగ్రత్త... Crypto Currency Trading పేరుతో మోసం చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు ...., సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్‌లకి సవాలు విసిరుతున్నారు. Youtube / Instagram/ Telegram లలో Crypto Currency / Stock marketing కు సంబంధించిన Videos చూసిన వారు ఆ Videos క్రింద అందుబాటులో ఉన్న ఫోన్ నెంబర్‌కి సంప్రదించిన లేదా ఫాలోలో క్రిప్టో కారెన్సీ ట్రేడింగ్ కు సంబంధిత పేజెస్ ని లైక్ చేయటం , ఫాలో అవ్వటం లేదా కామెంట్స్ చేసి సైబర్ నేరగాళ్ళు వలలో మనము చికుకున్నట్లే. వాళ్ళు చెప్పినట్లు చేసిన క్రిప్టో కారెన్సీ ట్రేడింగ్ ద్వార మంచి లాభాలు వస్తాయని 10% ప్రాఫిట్ వాళ్ళకి ఇవ్వాలని మనల్ని నమ్మించి. క్రిప్టో కారెన్సీ ఎలా కొనాలో నేర్పించి, మనమే క్రిప్టో కారెన్సీ కొని సైబర్ నేరగాళ్ళు అకౌంట్ కు డిపాజిట్ చేసేలా చేస్తారు. అనంతరం మనము ఇన్వెస్ట్ చేసిన అమౌంట్ వాళ్ళు పంపించిన లింక్ క్లిక్ చేయగా వర్చ్యువల్‌గా కనిప్పించే విధంగా చేస్తారు. మంచి ప్రాఫిట్ వచ్చినట్టు చూపిస్తారు. బాధితుడు సదరు వ్యక్తికి సంప్రదించగా విత్‌డ్రా చార్జస్ / జియస్‌టి / లేట్ అని రకరకాలగా మాయమాటలు చెప్పి మరింత డబ్బులు కాజేస్తారు మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనార్హం.

నేర విధానం వివరంగా :

1. మనం ఎవరైన క్రిప్టో కరెన్సీ / ట్రేడింగ్ కు సంబంధించి యూట్యూబ్ / ఇన్‌స్టాగ్రామ్/ టెలిగ్రామ్ వీడియోస్ ఫాలో అయ్యి అందులో మీకు ఎమైన డౌట్స్ ఉంటే కాంట్యాక్ట్ చేయండి అని కామెంట్స్ పెట్టే వారిని కాంట్యాక్ట్ చేసినట్లు అయిన మనం సైబర్. నేరగాళ్ళు వలలో చిక్కుకున్నట్లే.

2. ఆవిధంగా కాంట్యాక్ట్ అయిన వ్యక్తి వాళ్ళు చెప్పినట్లు చేస్తే క్రిప్టో కారెన్సీ ట్రేడింగ్ ద్వార మంచి లాభాలు వస్తాయని, వచ్చిన లాభాంలో 10% వాళ్ళకి ఇవ్వాలని మనం నమ్మేవిధంగా వివరిస్తారు.
3. అనంతరం ఇందులో పెట్టుబడి పెట్టాలంటే ముందుగా Binance/ CoinDCX/ ect లాంటి క్రిప్టో కారెన్సీ ట్రేడింగ్ యాప్స్ డౌన్‌లోడ్ చేసి అందులో రిజిస్టర్ అవ్వమని చెబుతారు.
4. ఇవి జెన్యూన్ అప్స్ కావున బాధితుడు సైబర్ నేరగాడు చెప్పినది నిజమని నమ్మి Binance లాంటి క్రిప్టో వ్యాలేట్ యాప్స్ లో రిజిస్టర్ అవుతారు.
5. అనంతరం సైబర్ నేరగాడు బాధితునితో Binance App లో బిట్‌కాయిన్/ యూయస్‌డిటి/ బైనాన్స్ కాయిన్ ఈ లాంటి క్రిప్టో కారెన్సీ ని కొనిపించి వాటిని సైబర్ నేరాగాడుకి సంబంధించిన ఫేక్ అకౌంట్ లోకి కి డిపాజిట్ చేయమంటాడు.
6. సైబర్ నేరగాడు బాధితునికి ఒక ఫేక్ లింగ్ పంపించి అందులో రిజిస్టర్ అవ్వండి మీరు ఇన్వెస్ట్ చేసిన అమౌంట్ మరియు మీకు వచ్చిన లాభాం కనిపిస్తుంది అని చెబుతాడు.
7. బాధితుడు ఆ లింక్ క్లిక్ చేసి రిజిస్ట్రేషన్ అవ్వగా అందులో మంచి లాభాలు వస్తున్నట్లు వర్చ్యువల్‌గా అమౌంట్ డిసిప్లే అవుతుంది.
8. బాధితుడు ఆ అమౌంట్ విత్ డ్రా చేయడానికి ప్రయత్నించగా, ఆ అమౌంట్ విత్‌డ్రా అవ్వదు. విత్‌డ్రా అవ్వడం లేదు కారణం ఏమిటి అని ఆ Fraudster ని అడగగా, అతను విత్‌డ్రా చేయాలంటే ముందుగా ఆ లింక్ లో తెలిపిన వెబ్‌సైట్స్‌కి విత్ డ్రా చార్జీస్ పే చేయాలని చెబుతారు.
9. ఆ అమౌంట్‌ని బాధితుడు పే చేసి మరల విత్‌డ్రా చేయటానికి ప్రయత్నిస్తాడు, అప్పటికి విత్‌డ్రా అవ్వకపోవటంతో GST Charges / Late Fee / etc Charges పేరుతో ఇంకొన్ని లక్షలు Fraudster మోసపురితంగా దోచుకుంటాడు.
10. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళు చేతిలో డబ్బులు వేసి మోసిపోతారు.



టాస్క్ ఫ్రాడ్ (రివార్డ్ పాయింట్ గెయినింగ్)



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి తస్మాత్ జాగ్రత్త... Advertisement ద్వార మనకు ఆశ చూసి టాస్కులు పేరుతో ఫ్రాడ్ చేసి డబ్బులు దోచుకుంటూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు ..... సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలిస్‌లకి సవాలు విసిరుతున్నారు. ఫేస్‌బుక్‌లో Advertisement పోస్టర్ వేస్తారు. ఆవి నచ్చిన వారు కాంటాక్ట్ అయితే వారికి టాస్కులు ఇస్తారు. డబ్బులు కొల్లగొడతారు, మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనార్హం... సైబర్ క్రైమ్ పోలీస్ ఉద్యోగులు చదువుకుంటున్న విద్యార్థులు, గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

నేర విధానం వివరంగా :

1. మొదటిగ సైబర్ నేరగాళ్ళు నేరం చేయటానికి సోషల్ మీడియా ప్లాట్‌ఫామ్ అయినటువంటి ఫేస్‌బుక్, ఇన్‌స్ట్రాగ్రామ్, వాట్సాప్, టెలిగ్రామ్ నందు అడ్వర్టైజ్‌మెంట్స్ రూపంలో ప్రజలకు వల విసురుతూ ఉంటారు.
2. అడ్వర్టైజ్‌మెంట్స్ చూసి ఎవరైతే రెస్పాండ్ అవుతారో వారికి రివర్స్ పాయింట్స్ సాధిస్తే మీరు అడ్వర్టైజ్‌మెంట్స్ చూసినట్లుగా “ఫూచర్ కిడ్స్ మోడలింగ్” కి మీ పిల్లలు సెలెక్ట్ అవుతారు అని చెపుతారు.

3. బాధితుడు అది నిజం అని నమ్మి ఏమి చేయాలి అని ఫేస్‌బుక్ మెసెంజర్ లేదా ఇతరత్రా ద్వారా సంప్రదిస్తాడు.

4. తరువాత Fraudster బాధితుడుకి ఒక లింక్ పంపిస్తాడు అందులో చాలా మంది ప్రముఖులు ఫోటోస్ ఉంటాయి అని ఫాలో అవ్వమని చెపుతారు.

5. బాధితుడు అది నిజం అని నమ్మి అదే విధంగా చేస్తాడు. తరువాత Fraudster మీరు అయిన వాటికి రివర్స పాయింట్స వస్తాయి అవి మీరు టెలిగ్రామ్ నందు చూడాలి అని చెప్పి ఒక టెలిగ్రామ్ ID ఇచ్చి జాయిన్ అవ్వమని చెప్పుతారు. తరువాత బాధితుడు యొక్క బ్యాంక్ అకాంట్, పాన్ కార్డు, పాస్‌ఫ్టోర్ట్ సైజు ఫోటో మరియు ఫోన్ నెంబర్ పంపమని అడుగుతారు.

6. బాధితేడుకి మొదటి పంపిన లింక్ ద్వారా ఫోటోస్‌ని లైక్ చెయ్యమంటారు అందుకు గాను ఒక ఒక లైక్ కి రూ. 50/– చప్పున రూ. 150/– నుంచి రూ. 300/– రూపాయలు వరకు బాధితుడు అకౌంట్‌లో జమ చేస్తారు. అలానే రివర్స్ పాయింట్స్ 10 నుంచి 20 కలుపుతారు అని టెలిగ్రామ్ ద్వారా చూపిస్తారు.

7. తరువాత లైక్స్ అవ్వగానే మార్చెంట్ టాస్క్ చెయ్యమని చెప్పుతారు అలా చేస్తే ఎక్కువ పాయింట్స్ వస్తాయి అప్పుడు మీకు సెలెక్ట్ అవుతారు అని చెపుతారు. బాధితుడు అది నిజం అని నమ్మి రూ. 2000/– రూపాయలుతో Fraudster పంపిన పేమెంట్స్ లింక్, యూపిఐ, ఐడి లేదా వ్యాలేట్స్ పంపిస్తారు.

8. అలా చేసిన వెంటనే Fraudster మరో టాస్క్ ఇవ్వడం జరుగుతుంది. ఆ టాస్క్ రూ. 5000/– తో కంప్లీట్ చేయగానే పాయింట్స్ 20 నుంచి 40 కలిపినట్టు చూపిస్తారు. అలానే కమిషన్‌తో కలిపి మొత్తం రూ. 9100/– రూపాయలు బాధితుడు అకౌంట్‌లో జమ చేశారు.

9. అ టాస్క్‌లు పూర్తి చేసిన తరువాత మీరు Upgrade అయ్యారు VIP టాస్క్ గ్రూప్ లో జాయిన్ అయి ఇంకా ఎక్కువ టాస్కు చేయాలి అప్పుడు రివర్స్ పాయింట్స్ 100 చేరుకొని మీరు సెలెక్ట్ అవుతారు అని చెపుతారు.

10. VIP గ్రూప్‌లో అని చెప్పి మరోక టెలిగ్రామ్ ఐడి ఇచ్చి జాయిన్ అవ్వమని చెపుతారు మరియు ఒక స్పెషల్ ట్యూబర్ గైడర్ గా ఉంటారు అని చెపుతారు దాని తరువాత బాధితుడుతో కలిపి ఆ గ్రూప్‌లో 5 నుంచి 6 మంది సభ్యులు వుంటారు.

11. మొత్తం ఆ గ్రూప్‌లో ఉన్న ఆ సభ్యులు అందరికి టాస్క్ ఇవ్వడం జరుగుతుంది. ఒకోక్క టాస్క్ రూ 1,00,000/- నుండి రూ. 10,00,000/- వరకు టాస్క్ అడమని ఇస్తారు. దినికిగాను వారికి ఫేక్ వైబ్‌సైట్ క్రియేట్ చేసి Virtual User ID మరియు Password ఇస్తారు.

12 వారు ఇన్వెస్ట్ చేసినటు వంటి అమౌంట్ Virtual ID లో కమిషన్‌తో కలిపి డిస్ప్లే అవుతుంది. మరియు టాస్క్‌లు కూడా కనిపిస్తాయి. కానీ వారికి అకౌంటులో మాత్రం డబ్బులు జమకావు. డబ్బులు జమ అవ్వలి అంటే ఇచ్చిన టాస్క్‌లు అని కంప్లీట్ అవ్వలని చెపుతారు.

13. టాస్కు అన్నీ కంప్లీట్ చేసిన సరే మేము చెప్పిన విధంగా మీరు చేయలేదు కాబట్టి ఇంకొన్ని టాస్క్‌లు చేయాలి అని చెపుతారు.

14. మళ్ళీ అమౌంట్ పే చేసి టాస్క్ కంప్లీట్ చేసిన తరువాత కూడ టాస్క్‌లో Errors వచ్చాయి అని చెప్పి యీ యూసర్ వాలెట్‌లో వున్న మైనస్ వున్న అమౌంట్‌ని మళ్ళీ పే చేయమని చెప్పుతారు.

15. చెప్పిన టాస్క్‌లు చేసిన తరువాత కూడా మీరు చేసిన టాస్కు, ఇన్‌టైమ్‌లో చేయలేదు అని చెప్పి మీ అకౌంటు CIBIL స్కోర్ తక్కువ ఉంది. కనుక మీరు మళ్ళీ పే చేయమని చెప్పుతారు.

16. అలా టాస్కు అన్నీ కంప్లీట్ అయినా తరువాత మీ డబ్బు విత్ డ్రా చేయాలి అంటే 30% CGT(Cash Gain Task) టాక్స్ పే చేయాలి అని చెప్తారు. మళ్ళీ మీ అకౌంటు పే రీజ్ లో ఉంది అని చెప్పి అది unfreeze చేయాలి అంటే కొంత అమౌంట్ పే చేయాలి అని చెపుతారు.

17. ఈ విధంగా బాధితుడు సైబర్ మొసగాళ్ళు చేతిలో డబ్బులు వేసి మోసమోతారు.

18. అలానే బాధితుడు ఎకౌంటులో వేసిన డబ్బులు కూడా మోసపోయిన వారితోనే వేయిస్తారు అందువల్ల మోసపోయిన వారు కంప్లెయింట్ ఇచ్చిన వెంటనే బాధితుడి బ్యాంకు అకౌంటు కూడా Freeze అవుతుంది.

పార్ట్‌టైమ్ జాబ్ ఫ్రాడ్ / ఆన్‌లైన్ జాబ్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి తస్మాత్ జాగ్రత్త... పార్ట్‌టైమ్ జాబ్/ టాస్కులు పేరుతో చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు..... సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్‌లకి సవాలు విసురుతున్నారు. వాట్సప్‌లో సందేశం పంపిస్తారు టాస్కులు ఇస్తారు డబ్బులు కొల్లగొడతారు మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడటం గమనార్హం. సైబర్ క్రైమ్ పోలీస్ స్టేషన్ లో విపరీతంగా క్రైమ్ రేట్ పెరుగుతుంది కారణం చదువుకున్నవారు ముఖ్యంగా సాఫ్ట్‌వేర్ ఉద్యోగులు చదువుకుంటున్న విద్యార్థులు, గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

నేర విధానం వివరంగా :

1. మొదటిగా సైబర్ నేరగాళ్ళు నేరం చేయడానికి సోషల్ మీడియా ప్లాట్‌ఫామ్ అయినటువంటి వాట్సాప్, టెలిగ్రామ్, ఫేస్‌బుక్, ఇన్‌స్టాగ్రామ్ నందు అడ్వర్టైజ్‌మెంట్ మరియు మెసేజెస్ రూపంలో ప్రజలకు వల విసురుతు ఉంటారు.
2. మెసేజెస్ గాని యాడ్స్ గాని చూసి ఎవరైతే రెస్పాండ్ అవుతాదు వారకి కమిషన్ ఆశ చూపిస్తూ కమిషన్ బేస్డ్ టాస్క్ గేమ్స్ క్రింద వారి రిక్రూట్ చేసుకునే విధంగా ఫేక్ వెబ్‌సైట్స్ డిజైన్ చేయబడునుతుంది.
3. బాధితుడుకి వాట్సాప్ లో రోజుకి రూ. 2,000/- నుండి రూ. రూ 4,000/- వరకూ ఇంటి వద్దనే ఉండి డబ్బులు సంపాదించవచ్చు అని మెసేజె వస్తుంది.

4. మొదటిగా ఫేరీ టాస్క్ అని చెప్పి యూట్యూబ్ లో వీడియోస్ లైక్, షేర్ సబ్‌స్క్రైబ్ చేయమని హుటల్స్ కి రివ్యూ ఇవ్వడం, ఈ – కామర్స్ (amazon, Flipkart, ebay, meshoo) లో ఉన్న Products రేటింగ్స్ ఇవ్వడం, సినిమా టికెట్స్ బుకింగ్ బాక్స్ ఆఫీసుకి రివ్యూ ఇవ్వడం అని చెప్తారు.
5. ఎవరైతే రెస్పాండ్ అవుతారో వారికి Telegram App లో జాయిన్ అవ్వమని చెప్పి వారియొక్క టెలిగ్రామ్ ఐడి ఇచ్చి జాయిన్ అవ్వమని చెప్పుతారు. తరువాత బాధితుడు యొక్క Bank Account, Pancard, Passport Size Photo మరియు ఫోన్ నెంబర్ పంపమని అడుగుతారు.
6. బాధితుడుకి మొదటిగా 4 షేర్ టాస్క్ ఇస్తారు. ఒకోక్క టాస్క్ గాను రూ. 25/– చప్పున రూ. 200 నుంచి రూ. 500/– రూపాయలు వరకూ బాధితుడు అకౌంట్‌లో జమ చేస్తారు.
7. 4 ఫ్రీ టాస్కులు అవ్వగానే ప్రిపేయిడ్ టాస్క్ చెయ్యమని చెప్పుతారు అలా చేస్తే ఎక్కువ కమిషన్ వస్తుంది అని చెపుతారు. బాధితుడు అది నిజం అని నమ్మి రూ. 500/– రూపాయలుతో Fraudster పంపిన Payment Link, UPI ID లేదా Wallets పంపిస్తారు.
8. అలా చేసిన వెంటనే Fraudster మరో 5 టాస్కు ఇవ్వడం జరుగుతుంది. ఆ టాస్క్ కంప్లీట్ చేయగానే కమిషన్‌తో కలిపి మొత్తంగా రూ. 800/– రూపాయలు బాధితుడు అకౌంట్‌లో జమ చేస్తారు.
9. అధిక మొత్తంలో కమిషన్ ఇన్కమ్ ఇంకా కావాలి అంటే ఎక్కువ మొత్తం లో రీచార్జి చేయాలి అని చెపుతారు అది రూ. 5,000/– రూపాయలు నుండి రూ 20,000/– రూపాయలుతో రీఛార్జ్ చేయమని చెపుతారు. బాధితుడుకి డబ్బులు పంపిన వెంటనే 10 టాస్కులు ఇచ్చి అవి కంప్లీట్ చేయమని చెపుతారు.
10. వారు ఇచ్చిన 10 టాస్క్‌లో కంప్లీట్ అవ్వగానే బాధితుడుకి అకౌంటులో డబ్బులు కమిషన్‌తో కలిపి వేస్తారు.
11. మీరు VIP గ్రూప్ మెంబర్ గా సెలక్ట్ అయ్యారు అని చెప్పి మరొక్క టెలిగ్రామ్ ఐడి ఇచ్చి జాయిన్ అవ్వమని చెపుతారు మరయు ఒక స్పెషల్ ట్యూబర్ Guider గా ఉంటారు అని చెపుతారు, దాని తరువాత బాధితుడు తో కలిపి ఆ గ్రూప్‌లో 5 నుంచి 6 మంచి సభ్యులు ఉంటారు.

12. మొత్తం ఆ గ్రూప్‌లో ఉన్న ఆ సభ్యులు అందరికీ టాస్క్ ఇవ్వడం జరుగుతుంది. ఒకోక్క టాస్క్ రూ. 1,00,000/- నుండి రూ. 10.00.000/- వరకూ టాస్క్ అడమని ఇస్తారు. దినికిగాను వారికి ఫేక్ వేబ్‌సైట్ క్రియేట్ చేసి Virtual User ID మరియు Password ఇస్తారు.
13. వారు ఇన్వెస్ట్ చేసినట్టు వంటి అమౌంట్ Virual ID కమిషన్‌తో కలిపి డిస్ప్లే అవుతుంది మరియు టాస్క్‌లు కూడా కనిపిస్తాయి. కానీ వారికి ఆకౌంటులో మాత్రం డబ్బులు జమ కావు . డబ్బులు జమ అవ్వలి అంటే ఇచ్చిన టాస్క్‌లు అన్ని కంప్లీట్ అవలని చెపుతారు.
14. టాస్కు అన్నీ కంప్లీట్ చేసిన సరే మేము చెప్పిన విధంగా మీరు చేయలేదు కాబట్టి ఇంకొన్ని టాస్క్‌లు చేయాలి అని చెపుతారు.
15. మళ్ళీ అమౌంట్ పే చేసి టాస్క్ కంప్లీట్ చేసిన తరువాత కూడ టాస్క్‌లో Errors వచ్చాయి అని చెప్పి యీ యూసర్ వాలెట్‌లో వున్న మైనస్ వున్న అమౌంట్‌ని మళ్ళి పే చేయమని చెప్పుతారు.
16. చెప్పిన టాస్క్‌లు చేసిన తరువాత కూడా మీరు చేసిన టాస్కు, ఇన్‌టైమ్‌లో చేయలేదు అని చెప్పి మీ అకౌంటు CIBIL స్కోర్ తక్కువ ఉంది. కనుక మీరు మళ్ళీ పే చేయమని చెప్పుతారు.
17. అలా టాస్కు అన్నీ కంప్లీట్ అయినా తరువాత మీ డబ్బు విత్ డ్రా చేయాలి అంటే 30% CGT(Cash Gain Task) టాక్స్ పే చేయాలి అని చెప్తారు. మళ్ళీ మీ అకౌంటు పే రీజ్ లో ఉంది అని చెప్పి అది unfreeze చేయాలి అంటే కొంత అమౌంట్ పే చేయాలి అని చెపుతారు.
18. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళ చేతిలో రూ. 10,00,000/- నుంచి తాను నమ్మినంత వరకూ డబ్బులు వేసి మోసపోతారు.

పెడెక్స్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి తస్మాత్ జాగ్రత్త...FedEx కోరియర్ పేరుతో మోసం చేస్తున్న సైబర్ నేరగాళ్ళు. ఫేక్ ఫోన్ నంబర్స్‌తో మనకి ఫోన్ చేసి FedEx లో మీ పేరు మీద కొరియర్ బుక్ అయింది అని అందులో వివిద రకాల illegal Items వున్నాయి అని చెప్పి మనలని భయభ్రాంతులకు గురి చేసి వారి చెప్పిన అకౌంట్స్‌లో డబ్బులు వేయించుకొని మోసం చేస్తున్నారు.

నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడికి ఒక తెలియని ఫోన్ నెంబర్ నుంచి ఫోన్ వస్తుంది. అతి లిఫ్ట్ చేసిన తరువాత మేము FedEx Couries నుంచి ఫోన్ చెస్తున్నాము అని చెప్పి మీపేరు మీద ఒక పార్సెల్ ముంబాయి నుండి తైవాన్ వెళుతుండగా ముంబాయి ఎయిర్పోర్ట్‌లో కస్టమ్ వారు పట్టుకున్నారు. అందులో అక్రమ రవాణా వస్తువులు అయిన 5 ఫేక్ పాస్ పోర్ట్స్, 3 క్రిడెట్ కార్డ్స్, 200 గ్రా MDMA పవడర్ (synthatic Drugs) 3500 INR క్యాష్ ఉంది. దానిని కస్టమ్స్ వాళ్ళు ముంబాయి క్రైమ్ బ్రాంచ్‌కి అప్పగించారు అని చెబుతారు.
2. భాదితుడు నేను ఏమి కొరియర్ బుక్ చేయలేదు చెప్పగా, ఆ Fraudster మీ పేరు, ఆధర్ కార్డు నెంబర్ చెబుతాడు. ఆ వివరాలు అన్ని కరెక్ట్‌గా ఉండడంతో భాదితుడు కొంచం భయానికి గురి అవుతాడు.

3. సైబర్ నేరగాళ్ళు Open Source Intelligence పరికరాళ్ళుతో భాదితుడు యొక్క వివరాలు కలెక్ట్ చేయడం జరుగుతుంది. ఆ వివరాలులే భాదితుడికి చెపుతారు.

4. అనంతరం భాదితుడికి ఆ పార్సెల్ పై గల తైవాన్ అడ్రస్ మరియు పార్సెల్ వివరాలు చెప్పి నోట్ చేసుకోమని చెబుతారు.

5. తరువాత ముంబాయి క్రైమ్ బ్రాంచ్ వారికి లైన్ కలుపుతున్నాము. మీరు వారితో మాట్లాడండి అని చెప్పి వేరే వాళ్ళకు లైన్ కలుపుతారు అందులో walkie talkie sounds వినిపిస్తారు.

6. అంతట మరో Fraudster కాల్ లిఫ్ట్ చేసి ముంబాయి క్రైమ్ బ్రాంచి నుండి మాట్లాడుతున్నట్లు చెబుతాడు. భాదితుడు పేరు వివరాలు చెప్పగా ఆ Fraudster మీ పేరు మీద వచ్చిన పార్సెల్ గురించి అందులో గల illegal transporting items గురించి చెప్పి, దిని మీద FIR రిజిస్టర్ చేయాల్సి ఉంది అని చెప్పి, ఇతర వివరాల కోసం ఇన్స్పేక్టర్ గారితో మాట్లాడమని ఫోన్ వేరేవాళ్ళకి ఇస్తారు.

7. తరువాత ఇంకో Fraudster పోలీస్ ఇన్సెపెక్టర్ మాట్లాడుతున్నట్టు బాధితుడుతో మాట్లాడుతాడు. భాదితుడు ఎటువంటి పార్సెల్ పంపలేదని. తనకి illegal items గురించి ఎటువంటి అవగాహనా లేదని నిరపరాధివి అని చెప్పిన. ఆ Fraudster వినకుండా మీరు వెంటనే ముంబాయి క్రైమ్ పోలీస్ స్టేషన్ కు రావాలని చెబుతారు. బాధితుడు వేరే లోకేషన్‌లో ఉన్నాను అని చెప్పగా Whatsapp/Skype ద్వారా మిమ్మల్ని కనెక్ట్ చేస్తాము. మేము అడిగిన ప్రస్నలన్నింటికి కరెక్ట్‌గా సమాధానం చెప్పాలని మీరు ఒంటరిగా ఉండాలి ఎవరు మీ దగ్గరలో ఉండకుడదు అని ఇన్వెస్టిగేషన్ కు సపోర్టు చేయాలని లేదంటే మీరు, మీ ఫ్యామిలీ అంతటిని అరెస్ట్ చేయాల్సి ఉంటుందని బయపెడతారు.

8. బాధితుడుకి Whatsapp / skype ద్వారా వీడియో కాల్ చేస్తారు. అక్కడ పోలీస్ యూనిఫారంలో ఇన్సెక్టర్ రెస్‌లో Fraudster కనిపిస్తాడు.

9. బాధితునికి వివిధరకాల ప్రశ్నలు వేసి, బాధితుని యొక్క పూర్తి వివరాలు అతని బ్యాంకు ఖాతా మరియు బ్యాలెన్స్ వివరాలు తెలుసుకుంటారు. ఇంతలో సిబిఐ నుండి ఇన్వెస్టిగేషన్ అంత Confidential ఉంచడానికి అంగికరిస్తునట్లు అగ్రిమెంట్ వచ్చింది అని CBI పేరుతో ఒక అగ్రిమెంట్ కాపి బాధితునికి పంపుతారు. అది చూసి బాధితుడు ఇంకా బయపడతాడు.

10. తరువాత బాధితుడుతో ఇంకా FIR ఫైల్ చేయలేదని, మీరు ఎటువంటి పార్సెల్ పంపలేదు అంటున్నారు కావున మా ACP గారితో మాట్లాడండి అని ఫోన్‌కాల్ వేరే వాళ్ళకి ఇస్తాడు. అతను చాల సిరియస్‌గా మాట్లాడి వెంటనే FIR చేసి తనదగ్గర పెట్టమని చెబుతారు ఇన్స్పెక్టర్‌గా మాట్లాడిన వ్యక్తి ఇన్వెస్టిగేషన్‌కు సహకరిస్తున్నాడని బాధితునికి సపోర్ట్ చేసిన విధంగా మాట్లాడుతాడు.

11. అప్పుడు ఆ ACP సరిగా వెరిఫై చేయమని సూచనలు ఇస్తాడు.

12. మరల ఆ ఫేక్ ఇన్స్పెక్టర్ బాధితునికి RBI తో Financial వెరిఫికేషన్ చేయించాలి అని అది క్లియర్ అయితే మీకు ఇక మీదట ఎటువంటి సమస్య ఉండదని చెబుతాడు. దాని కోసం మీరు వాళ్ళు చెప్పిన బ్యాంకు అకౌంటుకి డబ్బులు పంపాలని, దానిని RBI Verify చేసి మీ అకౌంట్స్ మనీ లండేరింగ్, టెర్రరిస్ట్ Activities సంబంధించినది కాదా అని నిర్ధారిస్తుంది. అనంతరం వెంటనే 20 min మీ అమౌంట్ రీఫండ్ అవుతుంది అని చెబుతాడు.

13. అనంతరం ఒక Fake RBI లెటర్ పంపుతారు.

14. భాధితుడు అది నిజం అని నమ్మి తన దగ్గర ఉన్న డబ్బులు అన్ని వాళ్ళ చెప్పిన అకౌంట్‌కి Transfer చేస్తాడు.

15. ఈ విధంగా బాధితుడు సైబర్ మొసగాళ్ళు చేతిలో డబ్బులు వేసి మోసపోతారు.



CENTRAL BUREAU OF INVESTIGATION - INDIA

CONSENT TO TERMS OF CONFIDENTIALITY AGREEMENT

Name: PASARLA VARAHA VENKATA PRASAD

AADHAR ID :7730-4635-7599

SUBJECT:- MONEY LAUNDERING CASE, DRUG TRAFFICING, IDENTITY THEFT

The respondent, I amPASARLA VARAHA VENKATA PRASAD hereby makes a promise of confidentiality for the purpose of filing an investigation into the illegal money laundering case.

1. In accordance with the provisions of IPC section 198, 223 and 420 of the Criminal Law, the crime of official duties and the crime of leaking secrets are punishable by imprisonment for a term of not less than three years and not more than seven years. The party involved in the case PASARLA VARAHA VENKATA PRASADbefore the case is not investigated clearly, shall not disclose state secrets to any person

2. For violation of the national financial order law, involving financial money laundering cases, the parties involved in the casePASARLA VARAHA VENKATA PRASADduring the investigation, telecommunications public security due to the needs of the case, will be for the bank accounts and mobile phones used in his name, do the whole legality of listening, monitoring non-state agencies suspected of crime, transferred to the judicial authorities.

3. The person involved in the case before the case is closed, without reporting may not leave the country without permission, and may not leave the place of residence limited to, if there is a violation will be prosecuted for suspected fugitive crime, the maximum two years to three years in prison.

4. I have read all the above provisions of the confidentiality agreement and` I agree to cooperate fully with the handling of the case.

MUMBAI POLICE

Money Laundering Case in charge:
MILIND BHARAMBE IPS (DCP CYBER)

Date of issue: 05-03-2024

Investigation Unit: Central Bureau of investigation team

ACKNOWLEDGEMENT LETTER FROM FINANCIAL DEPARTMENT

RESERVE BANK OF INDIA

F .No. MINM/MBZO - I / 01 / 2023 Dated:-05.03.2024

MONEY LAUNDERING CASE :PASARLA VARAHA VENKATA PRASAD(7730 4635 7599)

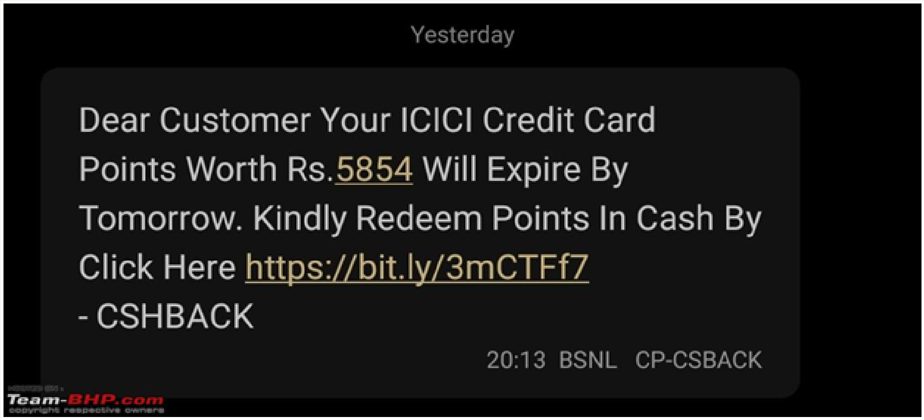
Indian Nationality Identity number 7730-4635-7599 money laundering case that person bank accounts to be verified with financial and CBI department of India and the person banks total amount to be verified by financial department and the amount will be verified and refunded within 30 minutes of investigation time. If having some illegal transactions in bank account we don't transfer the money back to the same bank account.

1. The case will be proceeding under this section shall be deemed to be judicial proceeding within the meaning of section 198 and section 223 of the Indian Penal code you will be processed under the session of judicial division which take one hour. This is approved by RBI and Crime branch Department.
2. The amount you sent for verification will be credited back to your account immediately within 30 minutes after the verification approved by the RBI.
3. This is an authorized transaction if you are making valid amount in your bank account and that transaction will be recognized by the government as legal or illegal.
4. If the amount is legal the payment will be rejected and your case will be canceled immediately.
5. The 9,56,740 amount is used as code of RBI in recognized software to detect and analysis the account is illegal or legal.

Department officials involving in this

1. MILIND BHARAMBE D.C.P (CYBER CRIME)
2. NITIN PATIL IPS (CRIME BRANCH COMMISSIONER)
3. GEORGE MATHEW IPS (FINANCIAL DEPARTMENT HEAD)
4. SHAKTI KANTA DAS FORMER IAS (SECRETARY OF MINISTRY)

రిడీమ్ పాయింట్స్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి తస్మాత్ జాగ్రత్త...Redeem Points పేరుతో Fraud చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు.... సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్‌లకి సవాలు విసురుతున్నారు. క్రెడెట్ కార్డు మరియు డిబెట్ కార్డు యొక్క రివార్డ్ పాయింట్ గడుపు త్వరలోనే ముగుస్తుందని కస్టమర్లకి మెసేజ్ పంపించి. అందులో పొందుపరిచిన లింక్ క్లిక్ చేసి క్రెడెట్ కార్డు మరియు డిబెట్ కార్డు వివరాలు భాదితుడు నమోదు చేయటం ద్వార డబ్బులు పోగొట్టుకుంటున్న సైబర్ భాదితుడు మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉ ఒడడం గమనార్హం... సైబర్ క్రైమ్ పోలీస్ స్టేషన్‌లో విపరీతంగా క్రైమ్ రేట్ పెరుగుతుంది కారణం చదువుకున్నవారు ముఖ్యంగా సాఫ్టవేర్ ఉద్యోగులు, పదవి విరమణ చేసేవారు గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడికి ఒక తెలియని ఫోన్ నెంబర్ నుంచి మెసేజ్ రావడం జరుగుతుంది.
2. దానిని తెరిచి చూడగా అందులో మీ యొక్క బ్యాంకు క్రెడెట్ లేదా డిబెట్ కార్డు రివార్డ్ పాయింట్స్ గడువు త్వరలో ముగుస్తుందని ఉంటుంది.
3. ఆ రివార్డ్ పాయింట్స్ ను నగదు గా మార్చుకొనుటకు ఈ లింక్ పై క్లిక్ చేయ్యాలని ఒక లింక్‌ను ఆ మెసేజ్‌లో పొందుపరుస్తారు.
4. బాధితుడుకు అది నిజం అని నమ్మేలా ఉంటుంది తర్వాత ఆ లింక్ పై క్లిక్ చెయ్యగానే బ్యాంకు వెబ్ పేజి ఒక ఫేక్ వెబ్ పేజి ఓపెన్ అయ్యి దానిలో మీ యొక్క క్రెడెట్ లేదా డిబెట్ కార్డు యొక్క వివరాలను తెలియపరచాలని ఉంటుంది.

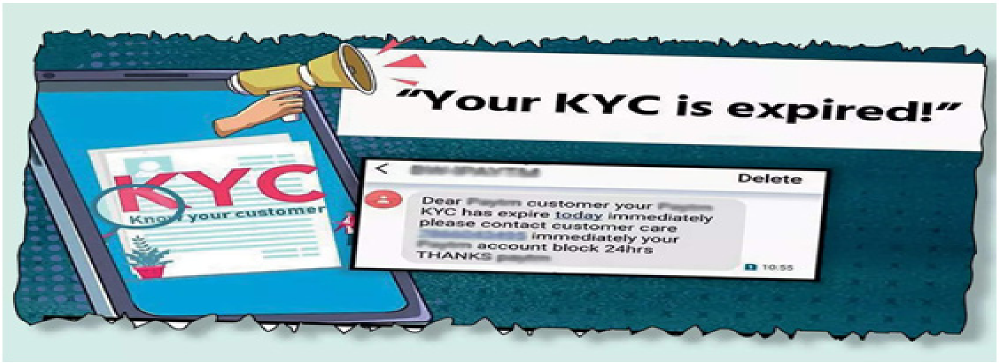
5. బాధితుడు రివార్డ్ పాయింట్స్‌ను నగదు గా మార్చలానే ఉద్దేశ్యంతో తన యొక్క క్రిడెట్ లేదా డెబిట్ కార్డు యొక్క వివరాలను ఆ వెబ్ పేజిలో టైపు చేస్తాడు.
6. దాని తర్వాత రివార్డ్ పాయింట్‌ను నగదు మార్చడానికి మీ ఫోన్ కు వచ్చిన OTP ను ఎంటర్ చెయ్యాలని ఉంటుంది.
7. భాధితుడు అది నిజం అని నమ్మి అలా OTP ని ఎంటర్ చేసిన వెంటనే భాదితుడి అకౌంట్ నుంచి డబ్బులు డెబిట్ అవుతాయి.
8. మరికొన్ని సందర్భాలలో బాధితుని ఫోన్ నుండి Fraudster నెంబర్ కి మెసేజ్ Fraudster చేయించుకొని OTP లని వచ్చే విధముగా చేసుకొని తద్వారా బాధితుడి ఎకౌంటు నుంచి డబ్బులు తస్కరిస్తారు.
9. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళు చేతిలో డబ్బులు వేసి మోసపోతాడు.

సైబర్ క్రైమ్ అవేర్నెస్ :-

యావన్మంది ప్రజానీకానికి సైబర్ క్రైమ్ పోలీసు వారి విజ్ఞప్తి తెలియని నెంబర్స్ నుంచి రివార్డ్ పాయింట్స్ వచ్చాయి లింకు క్లిక్ చేయండి అని మెసేజెస్ వస్తే వెంటనే డిలిట్ చేసేయండి, ఎలాంటి లినక్స్ క్లిక్ చేయవద్దు.



కెవైసి అప్‌డేట్ ప్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి తస్మాత్ జాగ్రత్త...KYC UPDATE పేరుతో Fraud చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు.... సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్‌లకి సవాలు విసురుతున్నారు. క్రెడెట్ కార్డు మరియు పాన్ కార్డు యొక్క KYC సమాచారం వివరాలు పూర్తిగా లేవని, వాటిని వెంటనే Update చేసుకోమని చెప్పి అది ఫేక్ అని తెలియని భాదితుడు. ఆ మెసేజ్‌లో పొందుపరచిన లింక్ క్లిక్ చేసి Credit Card లేదా Pan Card మరియు బ్యాంక్ ఖాతా వివరాలు భాదితుడు నమోదు చేయటం ద్వార డబ్బులు పోగొట్టుకుంటున్న సైబర్ భాదితుడు మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనార్హం... సైబర్ క్రైమ్ పోలీస్ స్టేషన్‌లో విపరీతంగా క్రైమ్ రేట్ పెరుగుతుంది కారణం చదువుకున్నవారు ముఖ్యంగా సాఫ్టవేర్ ఉద్యోగులు, పదవి విరమణ చేసేవారు గృహిణులు వారికి వస్తున్న మెసేజ్ సారిగా గమనించకుండా సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడికి ఒక తెలియని ఫోన్ నెంబర్ నుంచి మెసేజ్ రావడం జరుగుతుంది.
2. దానిని తెరిచి చూడగా అందులో మీ యొక్క బ్యాంకు క్రిడెట్ లేదా పాన్ కార్డు యొక్క KYC సమాచారం వివరాలు పూర్తిగా లేవని, వాటిని వెంటనే Update చేసుకోవాలని, లేదంటే మీ బ్యాంక్ ఖాతా లేదా క్రిడెట్ కార్డ్ బ్లాక్ అవుతాయని ఉంటుంది.
3. ఈ మెసేజ్ చూడగానే బాధితుడు బ్యాంఖ్ ఖాతా లేదా క్రిడెట్ కార్డ్ బ్లాక్ అవుతాయని నమ్మి. ఆ మెసేజ్ లో ఉన్నా లింకు పై క్లిక్ చేసి దానిలో ఒక కొత్త వెబ్ పేజీ, బ్యాంకు వారి సైట్ తో పోలి ఉన్నది ఓపెన్ అయ్యి దానిలో క్రిడెట్ కార్డు లేదా డిబెట్ కార్డు మరియు పాన్ కార్డు వివరాలను అడుగుతుంది.

4. దాని తర్వాత బాధితుడు ఆ వెబ్ పేజీలో తన క్రిడెట్ కార్డు లేదా డిబెట్ కార్డు మరియు పాన్ కార్డు వివరాలను టైపు చేస్తాడు.
5. ఆ తర్వాత బాధితుడికి OTP వస్తుంది దానిని ఆ వెబ్ పేజిలో ఎంటర్ చేయమని ఉంటుంది.
6. ఒక్క సారి బాధితుడు OTP ఎంటర్ చేయగానే బాధితుడి ఎకౌంటు నుంచి డబ్బులు డెబిట్ అవుతాయి.
7. మరికొన్ని సందర్భాలలో బాధితునికి ఫోన్ కాల్స్ ద్వారా నేరగాళ్ళు మీ యొక్క బ్యాంకు క్రిడెట్ కార్డు లేదా డిబెట్ కార్డు మరియు పాన్ కార్డు యొక్క KYC సమాచారం వివరాలు పూర్తిగా లేవని. వాటిని వెంటనే Update చేసుకోవాలని లేదంటే మీ బ్యాంక్ ఖాతా లేదా క్రిడెట్ కార్డు బ్లాక్ అవుతాయని చెబుతారు.
8. అది విన్న భాదితుడు నిజం అని నమ్ముతాడు, దాని తర్వాత ఆ ఫోన్లో మాట్లాడే వ్యాక్తి భాదితుడి whatsapp కు ఒక APK FIle ను పంపి దానిని వాళ్ళ ఫోన్‌లో ఇస్టాల్ చేసుకోమని చెబుతాడు.
9. ఆ తర్వాత భాతితుడికి ఆ APK File ఓపెన్ చేయమని చెబుతారు. ఆ APP ఒక రిమోట్ కంట్రోల్ APP దాని ద్వారా భాదితుడిని ఇంటర్నెట్ బ్యాంకింగ్ పాస్వర్డ్ లు మరియు UPI PIN తన ద్వారా ఆ ఇంటర్నెట్ బ్యాంకింగ్ మరియ UPI APP లను ఓపెన్ చేయించడం ద్వారా నేరగాళ్ళు మీ పాస్వర్డ్ తెలుసుకుంటారు.
10. ఆ తర్వాత రిమోట్ కంట్రోల్ APP ను వాడి బాధితుడి ఫోన్ ని కంట్రోల్ చేసి ఇంటర్నేట్ బ్యాంకింగ్ మరయు UPI App పాస్వర్డ్ ను వాడి, వారి ఫోన్ కి వచ్చిన OTP's బాధితుడి ఫోన్‌లో చూసి డబ్బులు దోచుకుంటాడు.

సైబర్ క్రైమ్ అవేర్నెస్ :

యావన్మంది ప్రజానీకానికి సైబర్ క్రైమ్ పోలీసు వారి విజ్ఞప్తి తెలియని నెంబర్స్ నుంచి క్రిడెట్ కార్డు లేదా డిబెట్ కార్డు మరియు పాన్ కార్డు యొక్క KYC అప్టేడ్ చేసుకోమని వచ్చే లింకులను, ఫోన్ కాల్స్ స్పందించవద్దని, ఒక వేళ మెసేజెస్ వస్తే వెంటనే డిలీట్ చేసేయండి, ఎలాంటి లింక్స్ క్లిక్ చేయవద్దు. మీకు ఎటువంటి మెసేజ్‌లు బ్యాంకు వారి హెడర్‌తో వస్తాయి. ఒక వేశ అనుమానం వస్తే బ్యాంకు వారిని సంప్రదించండి.



జాబ్ ఫ్రాడ్

సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి తస్మాత్ జాగ్రత్త...JOBSపేరుతో Fraud చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు.... సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్‌లకి సవాలు విసురుతున్నారు. కొంతమంది ఉద్యోగ ఉద్యోగ అవకాశం కోసం గాని లేక మెరుగైన ఉద్యోగ అవకాశల కోసం naukari.com, trimesjob.com నందు గారిResume ని అప్లోడ్ చేయడం ద్వారా బాధితుడికి ఫోన్ చేసి JOB ఇప్పిస్తామని మాయమాటలు చెప్పి నమ్మించి వారి వద్ద నుండి దఫదఫాలుగా వివిధ Charges రూపంలో డబ్బులు కాజేస్తున్నా సైబర్ నేరగాళ్ళు చేతిలో మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనావర్హం... సైబర్ క్రైమ్ పోలీస్ స్టేషన్‌లో విపరీతంగా క్రైమ్ రేట్ పెరుగుతుంది కారణం చదువుకున్నవారు ముఖ్యంగా సాఫ్టవేర్ ఉద్యోగులు, పదవి విరమణ చేసేవారు గృహిణులు వారికి వస్తున్న మెసేజ్ సారిగా గమనించకుండా సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

నేర విధానం వివరంగా :

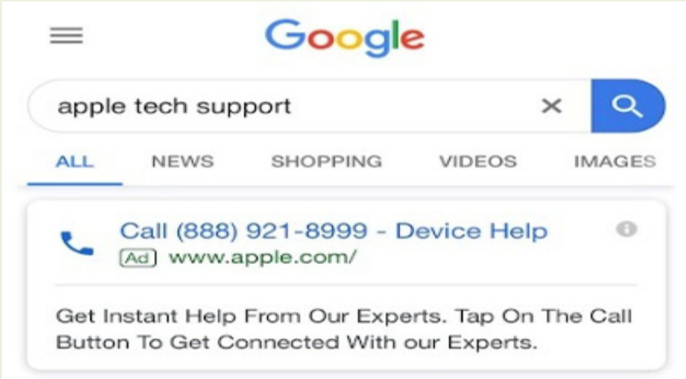
1. మొదటిగా భాదితుడికి ఉద్యోగ అవకాశం కోసం గాని లేక మెరుగైన ఉద్యోగ అవకాశాల కోసం ఆన్లైన్ website naukari.com, timesjob.com నందు Resume ని అప్లోడ్ చేస్తారు
2. తరువాత ఒక గుర్తుతెలియని ఫోన్ నెంబర్ నుండి భాదితుడికి ఫోన్ వస్తుంది. ఆఫోన్‌లో మాట్లాడే వ్యక్తి తను ఒక ప్రముక కంపెని నుంచి ఫోన్ నుంచి చేస్తున్నానని చెప్పి మీరుwebsite naukari.com, timesjob.com చేసిన Resume మా కంపెనీ వెరిఫేకేషన్ లో షార్ట్ లిస్టు అయ్యిందని, తరువాత Job యొక్క వివరాలు, జీతం వంటి విషయాల గురించి చెప్పి , మీరు స్వదేశంలో గాని, విదేశాలలో గాని Job చెయ్యడానికి సిద్ధంగా ఉన్నారా అని చెప్పి బాధితుడిని నమ్మిస్తారు.
3. భాదితుడి వారి మాటలు నమ్మి మరింత నమ్మిచేందుకు బాధితుడకి Whatapp లో బాదితుని పేరు మీద ప్రబుఖ కంపెని లెటర్ హెడ్ తో ఒక నకిలీ JOb సెలక్షన్ ఆర్డర్ తయారు చేసి దాని ఫోటును పంపుతారు.
4. ఆ తర్వాత భాదితుడుని మరింత నమ్మిచెందుకు బాధితుడుకు whatsapp లో బాధితుని పేరు మీద ప్రముఖ కంపెని లెటర్ హెడ్ తో ఒక నకిలి Job సెలక్షన్ ఆర్డర్ తయారు చేసి దాని ఫోటోను పంపుతారు.

5. దాని తర్వాత బాధితునికి ఫోన్ కాల్స్ ద్వారా గాని, Whatapp ఛాటింగ్ ద్వారా గాని ట్రైనింగ్ చేర్జస్, ఎంప్లాయ్ ప్రొఫైల్ ఫీజు, కన్నర్మేషన్ ఫీజు వెరిఫికెషన్ చార్లెస్ వీసా ప్రాసెస్ చార్జెస్ అని వివిధ Charges రూపంలో డబ్బులు చెల్లించాలని చెబుతారు.
6. దానికి బాధితుడు అతను చెప్పిన విధంగా డబ్బులను చెల్లిస్తాడు. అయినప్పటికి Job రాకపోవడంతో సైబర్ నేరగాళ్ళ చేతిలో మోసపోయానని భావిస్తాడు.
7. ఈ విధంగా బాధితడు సైబర్ మోసగాళ్ళు చేతిలో డబ్బులు వేసి మోసపోతారు.

సైబర్ క్రైమ్ అవేర్నెస్ :

యావన్మంది ప్రజానీకానికి సైబర్ క్రైమ్ పోలీసు వారి విజ్ఞప్తి ఆన్లైన్ లో అనాధికారిక website లలో Resume ని అప్లోడ్ చేయవద్దని, తెలియని నంబర్స్ నుంచి ఫోన్ చేసి JOB ఇప్పిస్తామని చెప్పే ఫోన్ కాల్స్ కి స్పందించవద్దని వారి మాటలు నమ్మి డబ్బులు చెల్లించవద్దు.

గూగుల్ సెర్చ్ కస్టమర్స్ కేర్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. మీరు కస్టమర్ కేర్ నెంబర్స్ గురించి గూగుల్ లో సెర్చ్ చేస్తున్నారా తస్మాత్ జాగ్రత్త... CUSTOMER CARE PHONE NUMBERS పేరుతో నకిలీ ఫోన్ నెంబర్స్ ను సైబర్ నేరాగాళ్ళు ఆన్లైన్ నమోదు చేసి వాటిద్వార Fraud చూస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు... కొంత మంది తమ సమస్య పరిష్కారం కోసం గూగుల్ లో కస్టమర్ కేర్ నెంబర్స్ వెతుకుతూ ఉంటారు. ఆన్లైన్లో నేరగాళ్ళు ముందుగానే నమోదుచేసిన నకిలీ ఫోన్ నెంబర్స్ మొదటిగా కనిపిస్తాయి ఆ నెంబర్స్ కు ఫోన్ చేసి వాళ్ళు నేరగాళ్ళు చెప్పినట్టుగా చేసి డబ్బులు పోగొట్టుకుంటున్న సైబర్ బాధితులు.

నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడు తన సమస్య పరిష్కారం కోసం గూగుల్లో కస్టమర్ కేర్ నెంబర్స్ వెతుకుతారు. దీనినే కొంతమంది సైబర్ నేరగాళ్ళు అదునుగా చూసుకొని కొన్ని నకిలి ఫోన్ నెంబర్స్ ను కస్టమర్ కేర్ నెంబర్స్ పేరుతో అనేఖల్లో నమోదుచేస్తారు.
2. భాదితుడు కస్టమరి కేర్ నెంబర్ కోసం సెర్చ్ చేసినప్పుడు వాళ్ళకి ఈ ఫేక్ ఫోన్ నెంబర్స్ కనబడుతాయి. దానికి అతడు అవి నిజమైన కస్టమర్ కేర్ నెంబర్గా భావించి ఆ నకిలీ ఫోన్ నెంబర్కు కాల్ చేస్తాడు.

3. అప్పుడు ఆ ఫోన్‌లో సైబర్ నేరగాళ్ళు మాట్లాడుతూ తాము సదరు కస్టమర్ కేర్ Representative అని చెప్పి బాధితుడు తో మాట్లాడి వారి సమస్య గురించి అడిగి తెలుసుకుంటారు. తరువాత వారి సమస్య పరిష్కారం కావాలంటే వారు పంపించిన లింక్స్ లేదా App ను డౌన్లోడ్ చేసుకోమని చెబుతాడు.

4. బాధితుడు అది నిజం అని నమ్మి ఆ APP ను ఫోన్లో ఇన్స్టాల్ చేసుకుంటారు. ఆ APP ఒక రిమోట్ కంట్రోల్ Access గలది. బాధితుడికి ఇంటర్నెట్ బ్యాంకింగ్ UPI APP లను ఓపెన్ చేయమని చెప్పి తద్వారా ఆ ఇంటర్నెట్ బ్యాంకింగ్ మరియు UPI APP యొక్క Pin మరియు పాస్వర్డ్‌ను తెలుసుకుంటారు.

5. ఆ తర్వాత రిమోట్ కంట్రోల్ APP ను వాడి భాదితుడి ఫోన్ ని కంట్రోల్ చేసి ఇంటర్నేట్ బ్యాంకింగ్ మరియు UPI APP యొక్క PIN మరియు పాస్వర్డ్‌ను వాడి వారి ఫోన్‌కి వచ్చిన OTP's భాదితుడి ఫోన్ లో చూసి డబ్బులు దోచుకుంటారు.

6. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళు చేతిలో మోసపోతారు.



OLX ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... OLX పేరుతో Fraud చూస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు... ఫేక్ OLX ప్రోఫైల్స్ తో తక్కువ ధరకి వస్తువులు పెట్టి మేము Central Reserved Force అయోనట్లు వంటి CISF, CRPF లో పనిచేస్తునము అని చెపుతారు. మాకు Transfer అయింది అందుకే వస్తువులు తక్కువకు ఇచ్చేస్తునము అని చెప్పి అడ్వాన్సు రూపంలో మన దగ్గర నుంచి వివిధ దఫాలుగా డబ్బులు వేయించుకుంటారు కానీ వస్తువులు పంపించరు. అలానే ఇంకో విధంగా వారి Army Process ప్రకారం మా QR Code ని స్కాన్ చేసి మీరు ఒక రూపీ పంపితే రెట్టింపు వస్తుంది అని అంటారు కానీ రాదు. మన నుంచే డబ్బులు వేయించుకొని మోసం చేస్తున్నారు. మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనార్హం... సైబర్ క్రైమ్ పోలీస్ స్టేషన్లో విపరీతంగా క్రైమ్ రేట్ పేరుగుతుంది. కారణం చదువుకున్నవారు ముఖ్యంగా సాఫ్టవేర్ ఉద్యోగులు, పదవి విరమణ చేసినవారు, గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడి అన్లైన్లో వస్తువులు కొందాం అని olx అప్లికేషను లో పెట్టిన ఫేక్ OLX ఫెర్ఫైల్స్ తో తక్కువ ధర కి ఉన్న వస్తువులు చూచి చాలా తక్కువ ధరకి వునై అని అనుకుంటాడు.
2. భాదితుడు అప్పుడు అందులో ఉన్న నెంబర్కి ఫోన్ ద్వారా కాంటాక్ట్ అవుతాడు.
3. అవతల వ్యక్తి వెంటనే నేను Central Reserved Force అయోనట్టు వంటి CISF, CRPF లో పనిచేస్తున్నాను నాకు రిసెంట్గా Transfer అయింది నేను

ఇప్పుడు షిఫ్ట్ అవ్వాలి తక్కువ ధరకి ఇచ్చేస్తున్న అని చెపుతాడు. తరువాత ఫేక్ ID కార్డ్స్ Whatsapp దార పంపుతారు.

4. భాదితుడు అదినిజం అని నమ్మిన తరువాత వస్తువుని చాలా తక్కువ ఇచ్చేస్తున్న చెప్పి మా Army Process ప్రకారం ముందు కొంత అడ్డాన్సు ఇవ్వాలి Trans port చేయుట గాను అని చెపుతాడు.
5. భాదితుడు అది నిజం అని నమ్మి Fraudster ఇచ్చిన అకౌంట్‌కి అమౌంట్ Trans port నిమ్మితం పంపుతాడు.
6. తరువాత కొంత GST Tax కూడా Pay చేయాలి అని ఇంకొంత అడ్వాన్సు అమౌంట్ పంపమని చెపుతాడు, భాదితుడు అలానే పంపుతాడు.
7. ఇంకొంత సమయం తరువాత వస్తువు Transport అయి కొంత దూరం వచ్చింది డ్రైవర్‌కి కొంత అడ్వాన్సు ఇవ్వాలి అని చెప్పి ఇంకొంత డబ్బులు అడుగుతారు.
8. అల వివిధ దఫాలుగా డబ్బులు వేయిచుకుంటారు. కాని వస్తువులు పంపరు అలానే ఫోన్స్ ఆఫ్ చేస్తారు ఎంత ప్రయత్నించిన ఫోన్ అవ్వదు.
9. అప్పుడు బాధితుడు తను మోసపోయ అని గ్రహిస్తాడు.
10. అలానే ఇంకో విధంగా మనం ఎద్దైయిన వస్తువుని అమ్ముదము అని OLX లో పెడితే. ఒక తెలియని ఫోన్ నెంబర్ నుంచి ఫోన్ వస్తుంది అది లిఫ్ట్ చేసిన తరువాత మీరు ఆన్లైన్ OLX లో పెట్టిన వస్తువులు చూసాము మాకు నచ్చింది అని చెపుతారు.
11. వాళ్ళు Central Reserved Force అయోనట్టు వంటి CISF, CRPF లో పనిచేస్తునాను అని చెపుతారు ఫేక్ ID కార్డ్స్ Whatsapp ద్వారా పంపుతారు.
12. ఒక రేట్ ఫిక్స్ అయిన తరువాత మా Central Reserved Force అమోనట్టు వంటి CISF, CRPF లో ఒక Process ఉంది దాని ప్రకారం చేయాలి అని అంటాడు.
13. ఒక QR CODE పంపి ఒక రూపయ్ పంపించమని చెబుతారు దానికి రెట్టింపు పై రెండు రూపాయలు మనకు వస్తుంది మళ్ళీ ఒక 50 రూపాయలు పంపించమంటారు ది రెట్టింపు పై వంద రూపాయలు వస్తుంది అ ప్‌రాసెస్ నిజమే అని నమ్మేలాగా చేస్తారు.
14. తర్వాత మన అడ్డాన్స్ ఎంత మాట్లాడుకున్నామో సుమారు ఒక 30000మాట్లాడకుంటే 30000 పంపమని చెబుతారు వేసితర్వాత మీకు రెట్టింపు అయ్యి అడ్వాన్స్ తో కలిపి వస్తుందని చెప్తారు. కాని మన అకౌంట్ నుంచి డబ్బు డెబిట్ అవుతే గానా ఆ అమోంట్ కి డబ్బులు రావు తర్వాత ఏంటని వాడిని అడుగుగా వాడు సార్ మీరు అల్‌రెడి ముందు ఒక రూపాయి వేసారు కదా అందువల్ల ఒక రూపాయి కట్ చేసి మిగతా 30 వేలు ఎంత అయితే ఉంటుంది. అంత అమౌంట్ వేయండి సార్ ఇక్కడ ఎర్రర్ చూసిస్తుందని అంటారు అది నిజమని డబ్బులు వేస్తాకా మళ్ళా రిటర్న్ రాదు.
15. మళ్ళీ ఫోన్ చేసేసరికి వాళ్ళు సిస్టం లో ఏదో ప్రబ్లం ఉంది ఎర్రర్ వస్తుంది. ఇంకోసారి ప్రయత్నించండి ఇంకోకసారి కూడా వేస్తాం మనకి తిరిగి రావు అప్పుడు బాధితులు ఇది మోసం అని అర్ధం చేసుకుంటారు.
16. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళు చేతిలో డబుబ్బలు వేసి మోసపోతారు.

ఇండియా బుల్స్ లోన్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... INDIAN BULLS LOAN లోన్ పేరుతో Fraud చూస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు... సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటూ సైబర్ పోల్ లకి సవాల్ విసిరుతున్నారు. లోన్ అవసరమైన వ్యక్తులకు ఇన్స్టెంట్ లోన్ ఇస్తామని మాయమాటలు చెప్పి వారి వద్ద నుండి దఫధఫలుగా డబ్బులు కాజేస్తున్నా సైబర్ నేరగాళ్ళు ఈ క్రమంలో మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనార్హం... సైబర్ క్రైమ్ పోలీస్ స్టేషన్లో విపరీతంగా క్రైమ్ రేట్ పేరుగుతుంది. కారణం చదువుకున్నవారు ముఖ్యంగా సాఫ్ట్వేర్ ఉద్యోగులు, పదవి విరమణ చేసినవారు, గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

నేర విధానం వివరంగా :

1. మొదటిగా లోన్ అవసరమైన వ్యక్తీ ఇంటర్నేట్‌లో లోన్ కోసం నెట్ లో సోదించినపుడు లేదా సామజిక మాధ్యమాలలో కనపడు లోన్స్ కి సంబందించిన ప్రకటనల పై క్లిక్ చెయ్యగా వారికి మొదటిగా INDIAN BULLS LOANS పేరుతో ఒక wiblink లేదా అప్లికేషను కనబడుతుంది.
2. దానిపై క్లిక్ చేస్తే Indian Bulls పేరుతో ఒక Website ఓపెన్ అవుతుంది. దానిలో ఆ వ్యక్తి లోన్ కోసం ఆప్లై చేయగా అతని యొక్క పేరు మరియు ఫోన్ నెంబర్ వివరములను అందులో టైప్ చేయమని అడుగుతుంది.
3. ఈ విధంగా చేసిన తర్వాత ఆ వ్యక్తికి ఒక తెలియని నెంబర్ నుంచి ఫోన్ వస్తుంది. తాను INDIAN BULLS LOANS నుంచి మాట్లాడుతున్నానని చెప్పి తన పేరు

మరయిుఉ కంపెనీ ID ఫోటోను Whatsapp ద్వారా పంపుతాడు. మీరు Loan కోసం అప్లై చేసారని మీకు ఆ లోన్ మంజూరు అయ్యిందని చెబుతాడు.

4. భాదితుడుకు అతడి మాటలు నమ్మి నిజంగానే లోన్ మంజూరు అయ్యిందని భావిస్తాడు. దాని తర్వాత వాళ్ళు బాధితుడిని నమ్మించడం కోసం అతని ఆధార్ పాన్ మరియు బ్యాంకు వివరాలను వారికి whatsapp ద్వారా పంపమని అడుగుతారు.
5. బాధితుడు వాళ్ళు చెప్పినట్టు గానే తన యొక్క ఆధార్, పాన్ మరియు బ్యాంకు ఖాతా వివరాలను వారికి వాట్సప్ ద్వారా పంపుతాడు.
6. ఆ తర్వాత భాదితుడుని మరింత నమ్మిచెందుకు అతని లోన్ మంజూరు అయ్యనట్టుగా ఒక నకిలీ ప్రమాణ పత్రలను అతనికి పంపుతాడు.
7. దాని తర్వాత ఫోన్‌లో ఉన్న వ్యక్తి బాధితుడుతో లోన్ సొమ్మును మీకు పంపడానికి మీరు ముందుగా Insurence Cherges కోసం కొంత సొమ్ము చెల్లించాలని చెబుతాడు.
8. దాని భాదితుడు అతను చెప్పిన విధంగా డబ్బులను చెల్లిస్తాడు. ఆ తర్వాత ఆ వ్యక్తి మరల EMI అడ్వాన్సు అని, TDS అని, RBI Charges అని రకరకాల పేర్లతో ఆ వ్యక్తి బాధితుడి వద్ద నుంచి డబ్బులని అడుగుతాడు.
9. ఇలా భాదితుడు తనకు లోన్ వస్తుందన్న ఆశాతో అతనికి పలుమార్లు అతను చెప్పినట్టుగా డబ్బులని వేస్తాడు.
10. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళ చేతిలో డబ్బులు వేసి మోసపోతారు.

సైబర్ క్రైమ్ అవేర్నెస్ :-

యావన్మంది ప్రజానీకానకి సైబర్ క్రైబ్ పోలీసు వారి విజ్ఞప్తి అన్లైన్ లో మరియు సామజిక మాధ్యమాలలో వచ్చే లోన్స్ సంబందించిన లింక్స్ మరియు ఫోన్ కాల్స్ కు స్పందిచావద్దని కోరుతున్నాము.



రెంటల్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... House Resnt పేరుతో Fraud చూస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు... సైబర్ నేరగాళ్ళు రోజుకో కొత్తపంథా ఎంచుకుంటూ సైబర్ పోల్ లకి సవాల్ విసురుతున్నారు. ఫేక్ ఫోన్ నెంబర్స్ తో మనకి ఫోన్ చేసి మేము Central Reserved Force అయోనట్టు వంటి CISF, CRPF లో పనిచేస్తున్నాము అని చెపుతారు Online లో మీరు పెట్టిన ఫ్లాట్ లేదా హౌస్ చూసాము మాకు Rajasthan, Haryana నుంచి వైజాగ్ Transfer అయింది రెంట్‌కీ మీరు పెట్టిన హౌస్ తీసుకుంటాము అని చెప్పి వారి Army Process ప్రకారం మా మీరు ఒక వన్ రూపి పంపితే రేటింపు అయి వస్తుంది అని అంటారు అలానే వస్తుంది. తరువాత రెంట్ అడ్వాన్సు కూడా అల పంపడి రెట్టింపు అయి వస్తుంది అంటారు కానీ రాదు అలానే ఇంకో విధంగా మా అకౌంట్స్ మీ UPI లో Add చేసుకొని మేము చెప్పిన విధంగా చేస్తే మీకు మేము పంపిన అడ్వాన్సు వస్తుంది అని చెప్పి మన దగ్గర నుంచే డబ్బులు వేయించుకొని మోసం చేస్తున్నారు. మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనార్హం... సైబర్ క్రైమ్ పోలీస్ స్టేషన్‌లో విపరీతంగా క్రైమ్ రేట్ పేరుగుతుంది. కారణం చదువుకున్నవారు ముఖ్యంగా సాఫ్ట్‌వేర్ ఉద్యోగులు, పదవి విరమణ చేసినవారు, గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

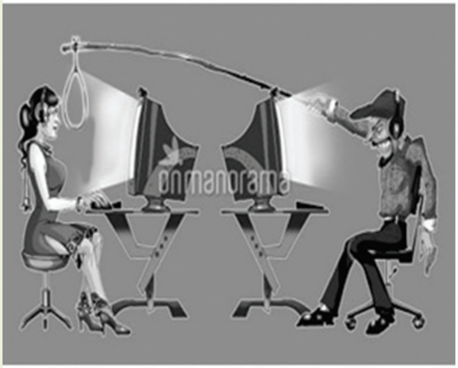
నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడికి ఒక తెలియని ఫోన్ నెంబర్ నుంచి ఫోన్ వస్తుంది అది లిఫ్ట్ చేసి తరువాత, మీరు అన్లైన్ (Magic Bricks, Housing. com, 99Acress) అప్లికేషను లో పెట్టిన ఫ్లాట్ లేది హౌస్ చూసాము అని చెపుతారు.
2. భాదితుడు అవును అని చెప్పిన వెంటనే నేను Central Reserved Force అయోనట్టు వంటి CISF, CRPF లో పనిచేస్తున్నాను నాకు రీసెంట్‌గా

Rajasthan, Haryana నుంచి వైజాగ్ Transfer అయింది నేను ఇప్పుడు షిఫ్ట్ అవ్వాలి అని చెపుతారు.

3. భాదితుడు నిజం అని నమ్మిన తరువాత హౌస్ ని వీడియో కాల్‌లో చూపమని చెప్పి హౌస్ నచ్చింది రెంట్ ఎంత కావాలి అడ్వాన్సు ఎంత ఇవ్వాలి అని మాట్లాడుతారు.
4. ఒక రేట్ ఫిక్స్ అయిన తరువాత Central Reserved Force అయోనట్టు వంటి CISF, CRPF లో ఒక Process ఉంది దాని ప్రకారం చేయాలి అని అంటాడు.
5. అందులో మొదటిగా ఒక రూపాయి పంపించమని చెబుతారు దానికి రెట్టింపు పై రెండు రూపాయలు మనకు వస్తుంది మళ్ళీ ఒక 50 రూపాయలు పంపించమంటారు అది రెట్టింపు పై వంద రూపాయలు వస్తుంది ఈ ప్రాసెస్ నిజమే అని నమ్మేలాగా చేస్తారు.
6. తర్వాత మన రెంట్ అడ్వాన్స్ ఎంత మాట్లాడుకున్నామో సుమారు ఒక 30,000 మాట్లాడుకుంటే 30000 పంపమని చెబుతారు వేసిన తర్వాత మీకు రెట్టింపు అయ్యి అడ్వాన్స్ తో కలిపి వస్తుందని చెప్తారు కానీ మన అకౌంట్ నుంచి డబ్బులు డెబిట్ అవుతే గాని ఆ అమౌంట్‌కి డబ్బులు రావు తర్వాత ఏంటని వాడిని అడుగగా వాడు సార్ మీరు ఆల్‌రెడీ ముందు ఒక రూపాయి వేస్తారు కదా అందవల్ల ఒక రూపాయి కట్ చేసి మిగతా 30 వేలు ఎంత అయితే ఉంటుంది అంత అమౌంట్ వేయండి సార్ ఇక్కడ ఎర్రర్ చూపిస్తుందని అంటారు అది నిజమని డబ్బులు వేస్తాం కానీ మళ్ళా రిటర్న్ రాదు.
7. మళ్ళీ ఫోన్ చేసే సరికి వాళ్ళు సిస్టం లో ఏదో ప్రబ్లం ఉంది ఎర్రర్ వస్తుంది ఇంకోసారి ప్రయత్నించండి ఇంకొక సారి కూడా వేస్తాం కానీ ఎన్నిసార్లు చేసినా సరే మన డబ్బులు పోవడం తప్ప మనకి తిరిగి రావు అప్పుడు బాధితులు ఇది మోసం అని అర్థం చేసుకుంటాడు.
8. రెండో విధంగా మీకు మేము పంపిన అడ్వాన్సు రావాలి అంటే మీరు మేము పంపిన అకౌంటుని మీ UPI Payments లో add చేసుకోండి అని చెపుతారు.
9. అది నిజం అని నమ్మి మన UPI లో అకౌంట్ add చేసుకున్న తరువాత మనం ఎంత అడ్వాన్సు అనుకునామో ఆ అమౌంట్ టైపు చేసి, recipeint దగ్గర మన పేరు add చేయమాని చేపుతాడు.
10. అలా చేసిన తరువాత భాదితుడు UPI Pin ఎంటర్ చేయవలసి ఉంటుంది. పిన్ ఎంటర్ చేసిన వెంటనే మన అకౌంట్ లోనించి డబ్బులు డెబిట్ అవుతాయి.
11. భాదితుడు వెంటనే fraudster కి అడిగితే లేదు మీ డబ్బులు మీకు refund అవుతాయి మొత్తం అడ్వాన్సు తో కలిపి ఇంకోసరి అలానే చేయండి అని అంటాడు.
12. భాదితుడు అది నిజం అని నమ్మి అలా చేసిన వెంటనే మరో సరి డబ్బులు కట్ అవుతాయి.
13. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళు చేతిలో డబ్బులు వేసి మోసపోతారు.

మ్యాట్రిమోనియల్ ఫ్రాడ్స్



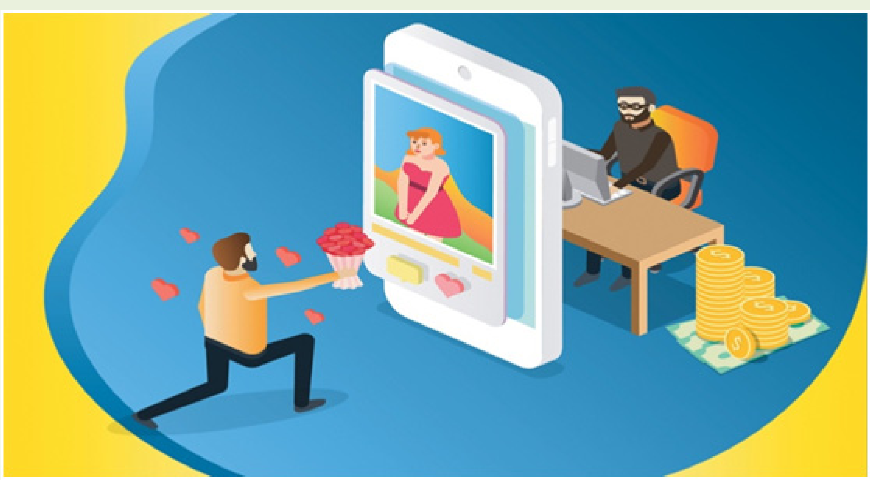


సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... మ్యాట్రిమోనియల్ వెబ్ సైట్స్ లో ఫేక్ ప్రొఫైల్ తో రిజిస్టర్ అయ్యి అమాయక అవివాహిత / విడో వ్యక్తులని మరిచయం చేసుకొని వివాహం చేకుంటామని నమ్మించి. విలువైన బహుమతులు పంపిస్తున్నట్లు ఏరా వేసి మోసగిస్తున్న సైబర్ నెరగాళ్ళు ఎక్కువ వయసు గల అవివాహితలు మరియు విడాకులుతీసుకొని మరో వివాహం కోసం మ్యాట్రిమోనియల్ వెబ్సైట్స్ లో రిజిస్టర్ చేసుకున్న వాళ్ళు ఎక్కువుగా మోసపోతున్నారు.

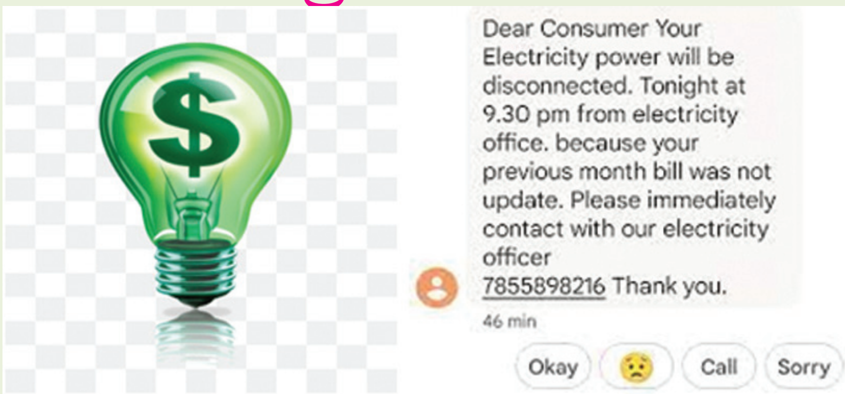
నేర విధానం వివరంగా :

1. పెళ్ళి సంబంధాలు చూసుకోను నిమత్త అవివాహిత వ్యక్తులు, విడోస్ గాని, Jeevansathi, shaadi.com, telugu matrimony etc మొదలైన మ్యాట్రిమోనియల్ Websites లో తమ యొక్క వ్యక్తిగత సమాచారం ఇచ్చి రిజిస్టర్ అవుతారు.
2. అవే మ్యాట్రిమోనియల్ వెబ్ సైట్స్ లో Fraudster Fake Profile తో రిజిస్టర్ అయ్యి ఎక్కువ వయస్సు గల అమాయక అవివాహిత లేదా Widow వ్యక్తులని టార్గెట్ చేసి మీ ప్రోఫైల్ చూసామని మీరు నచ్చారని ఛాటింగ్ చేసి పరిచయం చేసుకుంటారు. వాళ్ళు ఫారిన్ కంట్రిస్ లో మంచి ఉద్యోగం చేస్తున్నట్లు మిమ్మల్ని పెళ్ళి చేసుకుంటానని నమ్మిస్తారు.
3. భాదితులకి ఫారన్ నుండి విలువైన బహుమతు పంపిస్తామని నమ్మించి బాధితుల యొక్క చిరునామా తిసుకుంటారు. మిమ్మల్ని నమ్మించడానికి ఫేక్ బిల్ కూడా పంపిస్తారు. అందులో డైమాండ్ నేక్లాస్చ కొంత గోల్డ్ ఎక్కువ మొత్తంలో డాలర్స్ కరెన్సీ పంపిస్తున్నట్లు పెడతారు.

4. మూడు నాలుగు రోజులు తరువాత మీకు భాహుమతి అందినదా లేదా అని ఎంక్వయిరీ చేస్తారు
5. తరువాత మీకు ఒక ఫోన్ కాల్ వచ్చి డిల్లీ ఎయిర్ పోర్ట్ కస్టమ్స్ డిపార్టుమెంటు నుండి మాట్లాడుతున్నట్లు చెప్పి మీ పేరున ఒక పార్సెల్ వచ్చింది అని, మీ పేరు వివరాలు చెప్పి అది మిరా కాదా అని నిర్ధరించుకుంటారు. బాధితులు ఆ భాహుమతి తనకు వచ్చింది అని వారికి చెబుతారు.
6. ఆ తర్వాత ఆ పార్సెల్ తిసుకోడానికి కస్టమ్ చార్జెస్ పే చాయ్యాలని కొంత డబ్బు అకౌంటు లో వేయించుకుంటారు.
7. మరి కొంత సమయానికి మరో ఫోన్ కాల్ చేసి ఆ పార్సెల్ స్కాన్ చేయగా అందు ఎక్కువ మొత్తం లో ఫారన్ కరెన్సీ ఉంది. బంగారం ఉంది. రూలు ప్రకారం అంత డబ్బులు పార్సెల్ ద్వార పంపడానికి లేదు. ఇవన్ని మీకు ఎలా వచ్చాయి. మీ మీద FIR Register చేయాల్సి ఉంటుంది అని మిమ్మల్ని బయపేట్టే విధంగా మాట్లాడుతారు.
8. తరువాత అలా చేయకుండా ఉండాలంటే 3,4 లక్షలు కట్టాల్సి ఉంటుందని చెప్పి బాధితుల వద్ద నుండి వారు చెప్పిన అకౌంట్స్ లో డబ్బులు వేయించుకుంటారు.
9. తరువాత ఈ డబ్బులు మీ అకౌంట్‌లో వేయాలని చెప్పి మీ అకౌంట్ నెంబర్ డిటేల్స్ తీసుకుంటారు.
10. ఈ అమౌంట్ డైరెక్ట్ గా మీ ఆకౌంట్‌లో వేయటం కుదరదు, RBI ద్వార వేయాలి అని RBI Charges కట్టాలని, అమౌంట్ డాలర్స్ నుండి రూపాయలకు మార్చడానకి మరికొంత డబ్బు కట్టాలని భాదితుడు నుండి వివిధ Charges పేరు తో చాలా ఎక్కువ అమౌంట్ దోచుకుంటారు. భాదితుడు ఇదంతా నిజమని చాలా అమౌంట్ వస్తుంది అనే ఉద్ధేశ్యంతో డబ్బులు Fraudster కేసి మోసపోతాడు.



ఎలక్ట్రసిటీ బిల్ల్ ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... ELECTRICITY BILL పేరుతో Fraud చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు... సైబర్ నేరగాళ్ళు రోజోకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్ లకి సవాల్ విసిరుతున్నారు. మీ మొబైల్ నెంబర్లు మీరు ముందు నెల కరెంటు బిల్ కట్టలేదు ఈ రాత్రి 9 : 30 గం॥ లకు లకు మీ కరెంటు కనెక్షన్ అపేయడం జరుగుతుంది. అల కాకూడదు అంటే క్రింద వున్న నెంబర్‌కి కాల్ చేయండి అని మెసేజ్ వోస్తుంది అది చూసి మనం నిజం అని నమ్మి కాల్ చేస్తే అవతలి వ్యక్తి మీకు హెల్ప్ చేస్తాము అని మ్మించి మీతో కొన్ని రకాల remote applications డౌన్లోడ్ చేయించి వారు మన యొక్క ఫోన్ కంట్రోలర్ తీసుకంఉటా. తరువాత మీ యొక్క ఎలక్ట్రికల్ బిల్ అప్‌డేట్ చేస్తాము అని ఒక లింక్ పంపించి తద్వారా 10 రూపాయలు పేమెంట్ చేయమంటారు UPI transactions ద్వార మన అకౌంట్ లో ఉన్న amount కాళీ చేస్తారు. మోసపోతున్నవారిలో ఎక్కువగా చదువుకున్నవారు ఉండడం గమనార్హం.

నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడికి ఒక తెలియని నెంబర్ నుంచి మెసేజ్ వస్తుంది అందులో మీరు ముందు నెల కరెంటుబిల్ కట్టలేదు కావున మీ యొక్క కరెంట్ కనెక్షన్ ఈ రోజు రాత్రి 9 : 30 గం॥లకు నిలిపివెయబుడుతుంది. తదుపని వివరాల కోసం ఎలక్ట్రిసిటీ ఆఫీసర్ ను సంప్రదించండి అని ఒక మొబైల్ నెంబర్ మెసేజ్ పెడతారు.
2. భాదితుడు అవతలి వ్యక్తికి కాల్ చేయగా మేము ఎలక్ట్రిసిటీ డిపార్టుమెంటు నుంచి మాట్లాడుతున్నము మీకు ఏ విధముగా సహాయం చేయాలి అని అడుగుతారు అంతట భాదితడు తన యొక్క కరెంటు కనెక్షన్ కట్ చేస్తారు అని మెసేజ్ వచ్చినది ముదు నెల కరెంటు బిల్లును కట్టేసము అని నెప్పగా అందుకు అవతలి వ్యక్తి మీకు కట్టిన కరెంటు

బిల్లు మా యొక్క సిస్టం లో అప్డేట్ కాలేదు మేము చెప్పిన విధముగా చేయండి వెంటనే మీ సమస్య పరిష్కరిస్తం చెబుతారు.

3. అనంతరం ఆ వ్యక్తి బాధితుడితో మీకు whatsapp లో ఒక file పంపిస్తాము అది డౌన్లోడ్ చేసుకొని అందులో మీ వివరాలు అప్లోడ్ చేయండి అని చెప్పి Whatsapp ద్వార ఒక restdesk. Any Desk etc లాంటి రిమౌట్ అప్లికేషన్ గల APK ఫైల్‌ను పంపుతాడు.
4. బాధితేడే ఆ యొక్క APK File డౌన్లోడ్ చేసుకొని తన యొక్క confidential వివరాలు అప్లోడ్ చేస్తాడు.
5. మరల ఆ Fraudster బాధితునికి ఒక 10 రూపాయలు Phonepe/Google/ Paytm లాంటి UPI Platform ద్వారా పంపించండి మీ కరెంట్ అప్‌డేట్ అవుతుంది అని ఒక లింక్ పంపుతాడు.
6. బాధితుడు raudster పంపిన లింక్ ద్వార 10 రూపాయలు పంపిన వెంటనే బాధితుడు ఎంటర్ చేసిన password ను Fraudster తను పంపించిన రిమోట్ App ద్వార తెలుసుకొని అనంతరం Fraudster బాధితుడు అకౌంట్ నుంచి డబ్బులను వివిధ UPI Transactions ద్వార తన యొక్క అకౌంట్స్‌కి పంపించి దోచుకుంటాడు.
7. ఈ క్రమంలో బాధితుడికి OTP రాకుండ ఉండడం కోసం Fraudster యొక్క మొబైల్ నెంబర్‌కు Message Forward సెట్టింగ్‌ను Enable చేసుకుంటాడు.



మీషో ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... Meesho పేరుతో Fraud చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు... సైబనఖ నేరగాళ్ళు రోజోకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్ లకి సవాల్ విసిరుతున్నారు. ఆన్‌లైన్ షాపింగ్ వేబ్‌సైట్స్ అయిన Meesho కస్టమర్లకి ఫేక్ లక్కీ డ్రా క్యాంపెన్స్ పంపించి తర్వాత ఫోన్ కాల్ చేసి తాము Meesho కంపెనీ ప్రతినిధులుగా పరిచయం చేసుకొని మీరు లక్కీడ్రాలో లక్షల రూపాయలు విన్ అయ్యారు అని చెప్పి నమ్మించి, వివిధ టాక్స్ క్రింద డబ్బులు దండుకుంటున్న సైబర్ మొసగాళ్ళు మోసపోతున్న ఎక్కువగా చదువుకున్న వారు ఉండడం గమనార్హం..., సైబర్ క్రైమ్ పోలీస్ స్టేషన్ విపరీతంగా క్రైమ్ రేట్ పెరుగుతుంది. కారణం, చదువుకున్నవారు ముఖ్యంగా సాఫ్ట్‌వేర్ ఉద్యోగులు, పదవి విరమణ చేసినవారు గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

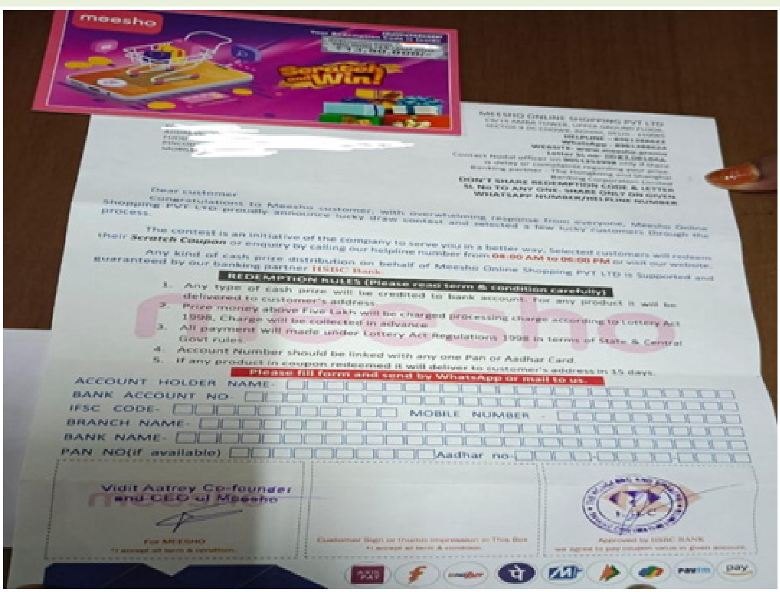
నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడికి ఒక తెలియని వారినుంచి పోస్ట్ రావడం జరుగుతుంది.
2. తెరిచి చూడగా అందులో Meesho కంపెనీ Scrach కార్డ్ ఉంటుంది. అది స్ర్కాచ్ చేయ్యగాఆ లక్కీడ్రా ద్వారా లక్షలంత రూపాయలు గెలుచుకున్నట్లు ఉంటుంది.
3. భాదితుడు అది నిజం అని నమ్మేలా ఉంటుంది. తరావ్వత దాని మీద ఉన్న నెంబర్‌కి కాంటాక్ట్ అమితే, అవతలి వ్యక్తి షాపింగ్ వెబ్‌సైట్స్ అయిన Meesho నుంచి మాటలు అడుతున్నాం అని చెప్పి, మీరు లక్కి డ్రా లో విన్ అయ్యారు చేసిన వివరాలు చెప్పటం చేత సదరు భాదితుడు నిజం అనుకునేలాగా చేస్తారు.
4. మొదటిగా డబ్బులు డిపోసిట్ చేయటానికి మీ అకౌంట్ డిటెయిల్స్ ఇవ్వండి అని చెప్పి అకౌంట్ ఇన్ఫర్మేషన్ తెలుసుకుంటారు.

5. తరువాత ట్యాక్స్ పే చేయాలి అని చెపుతారు అది నిజం అని నమ్మి మన UPI ద్వార వారు ఇచ్చిన అకౌంట్ కు అమౌంట్సు వెయ్యడం జరుగుతుంది.
6. అలా చేసిన తరువాత భాదితుడుకి ఇంక ఇతరితన ట్యాక్స్ ల పేరుతో డబ్బు కట్టాలి అని చెబుతారు. అలా చేస్తేనే మీ అమౌంట్ మీకు వస్తుంది అని చెప్పి చాలా డబ్బులు వేయించుకుంటాడు.
7. భాదితుడు వెంటనే Fraudster కి అడిగితే లేదు మీ డబ్బులు మీకు refund అవుతాయి మొత్తం లక్కీ అమౌంట్‌తో కలిపి ఇంకో సరి అలానే చేయండి అని అంటాడు.
8. భాదితుడు అది నిజం అని నమ్మి అలాచేసిన కానీ ఎటువంటి డబ్బులు కూడా భాదితుడు అకౌంటుకి రావు.
9. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళ చేతిలో డబ్బులు వేసి మోసపోతారు.

సైబర్ క్రైమ్ అవేర్నేస్ :-

యావన్మంది ప్రజానీకానికి సైబర్ క్రైమ్ పోలీసు వారి విజ్ఞప్తి Awareness Meesho, Amazon, Flipkart, naptool వంటి పలు అన్‌లైన్ షాపింగ్ వెబ్‌సైట్స్ నుంచి మీకు గిఫ్ట్ వచ్చింది కార్ గెలుచుకున్నారు వంటి offers ని నమ్మవద్దు మరియు Phonepay, Paytem, Google వంటి వాటినుంచి రిచార్జ్ పాయింట్స్ వచ్చాయి లింకు క్లిక్ చేయండి అని మెసేజెస్ వస్తే వెంటనే డిలీట్ చేసేయండి ఎలాంటి లింక్స్ క్లిక్ చేయవద్దు.



AEPS (ఆధార్ ఏనేబుల్డ్ పేమెంట్ సిస్టమ్) ఫ్రాడ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... AEPS (AADHAR ENABLED PAYMENT SYSTEM)పేరుతో Fraud చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు... సైబనఖ నేరగాళ్ళు రోజోకో కొత్తపంథా ఎంచుకుంటు సైబర్ పోలీస్ లకి సవాల్ విసిరుతున్నారు. కొంతమంది రిజిస్ట్రేషన్ లేదా ఇతర అవసరాలకి మంన వేసే వేలిముద్రలని సైబర్ నేరగాళ్ళ థర్డ్ పార్ట్ దగ్గర నుంచి దొంగలించి దానితో మన ఆధార్ లింక్ బ్యాంకు అకౌంట్ లో ఉన్న డబ్బును దొంగాలిస్తునాడు. మోసపోతున్న వారిలో ఎక్కువగా గృహిణులు, చిన్న వ్యాపారులుయ మధ్యవయసు గలవారు ఉండడం గమనార్హం. సైబర్ క్రైమ్ పోలీస్ స్టేషన్‌లో విపరీతంగా క్రైమ్ రేట్ పెరుగుతుంది.

నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడి రిజిస్ట్రేషన్ లేదా ఇతర అవసరాలకి తన యొక్క వెలిముద్ర Biometric థార్ట్ పార్టీ అప్లికేషన్‌లో వెస్తాడు.
2. తరువాత సైబర్ నేరగాళ్ళు ధర్డ్‌పార్టీ అప్లికేషను దగ్గర నుంచి ఆ యొక్క డేటాని దొంగలిస్తాడు.

3. భాదితుడి తన యొక్క బ్యాంకు అకౌంటుకు ఆధార్‌ను KYC లో భాగంగా అనుసందానం చేసికొని ఉంటాడు.

4. భాదితుడి అకౌంటు డబ్బులు తిసే మార్గంలో UPI, INB, ATM వాడుకొని డబ్బు తీసుకోవచ్చు అలాగే <u>AADHAR ENABLED PAYMENT SYSTEM</u> అనే పద్దతి ద్వారా కూడా డబ్బులు మన వెలిముద్రను ఉపయోగించి తీసుకొనవచ్చు.

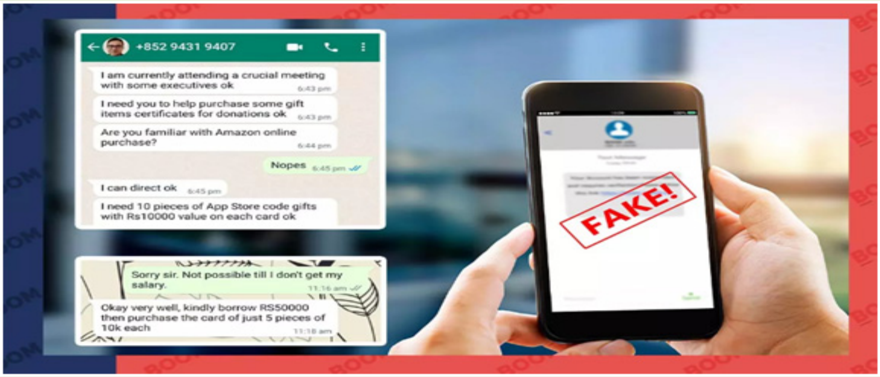
5. సైబర్ నేరగాళ్ళు ఆ దొంగిలించిన డేటా లో ఉన్న వేలిముద్రలను వాడుకొని ATM సౌకర్యం లేని రిమోట్ Village లో చిన్న చిన్న మినీ ATM (CSP) నడిపే వారితో భాదితుల అకౌంటు నుండి దొంగలించిన వేలిముద్రలను వాడుకొని డబ్బులు With drawal చేస్తున్నారు.

6. అయితే సాధారణంగా అందరి అకౌంటు కి (AADHAR ENABLED PAY MENT SYSTEM) అనే అప్షన్ అటోమేటిక్‌గా ఆక్టీవ్ అయ్యి ఉంటుంది.

7. ఇదే అవకాశాన్ని వాడుకొని సైబర్ భాదితుని అకౌంటు నుండి డబ్బులను AEPS పద్ధతి ద్వారా భాదితునికి తెలియకుండా వారియొక్క వేలిముద్రలను వాడి తిస్తున్నారు.

8. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళు చేతిలో డబ్బులు కోల్పోయి మోసపోతున్నారు.

వాట్సాప్ ఇంపర్సొనేషన్

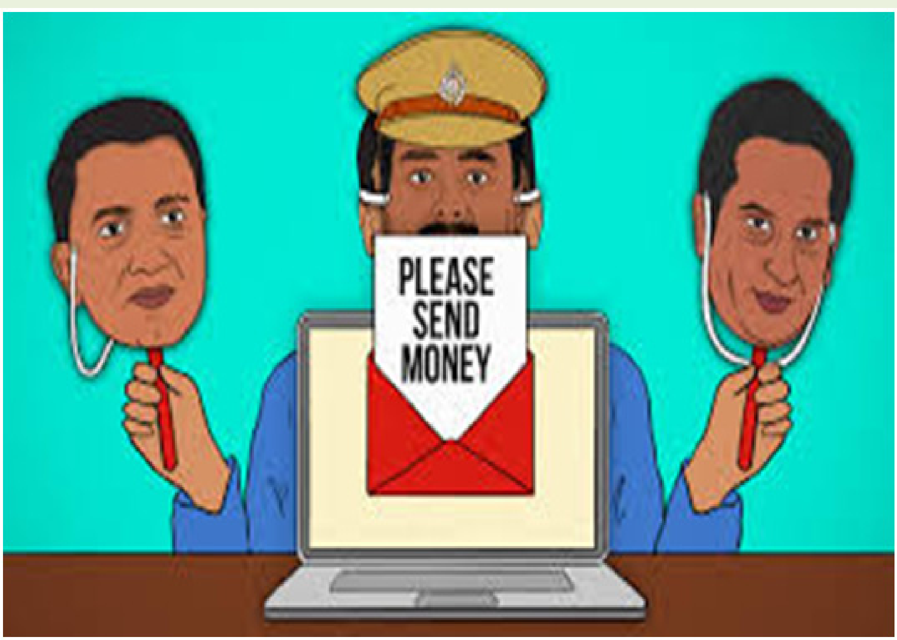


సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... WHATSAPP IMPERSONATION పేరుతో Fraud చూస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు..., WHATSAPP అప్లికేషన్ లో ఫేక్ నెంబర్‌తో ప్రముఖుల లేదా మనకు తెలిసిన వాళ్ళ ఫోటో DP (డిస్ప్లే పిక్చర్) గా ఉంచి మనకు Whatsapp ద్వార ఎమర్జెన్సీ ఉంది డబ్బులుకావాలి మళ్ళీ రిటర్న్ ఇచేస్త అని మెసేజ్ చేసినట్లు ఉన్నారో వారిని ఫోన్ ద్వార సంప్రదించకుండా డబ్బులు వేస్తామో తరువాత అది ఫేక్ అని తెలిసి మోసపోయం అని భాదితుడు గ్రహిస్తాడు. మోసపోతున్న వారిలో ఎక్కువగా చదువుకున్నవారే ఉండడం గమనార్హం... సైబర్ క్రైమ్ పోలీస్ స్టేషన్‌లో విపరీతంగా క్రైమ్ రేట్ పేరుగుతుంది. కారణం చదువుకున్నవారు ముఖ్యంగా సాఫ్టవేర్ ఉద్యోగులు, పదవి విరమణ చేసినవారు, గృహిణులు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.

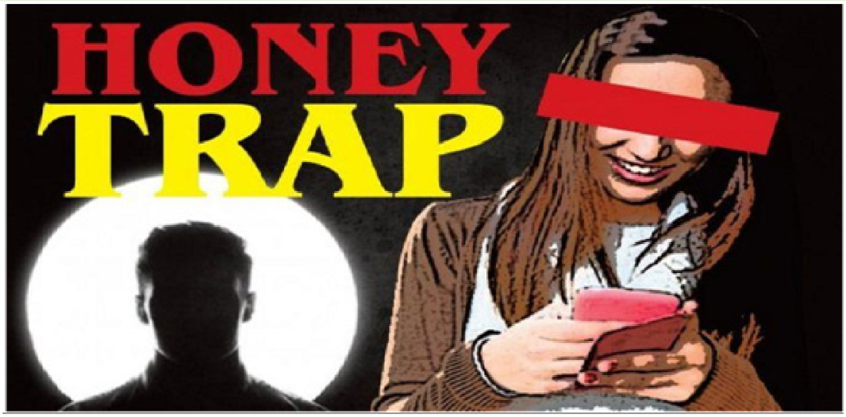
నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడి తెలియని Whatsapp నెంబర్ తెలిసిన వాళ్ళ ఫోటో DP (డిస్ప్లే పిక్చర్) తో ఒక మెసేజ్ వస్తుంది.
2. భాదితుడికి కొత్త నెంబర్ నుంచి మెసేజ్ రావటం వల్ల అవతలి వ్యక్తిని Whatsapp మెసేజ్ ద్వారా ప్రశ్నిస్తాడు.
3. అ మెసేజ్ ముఖ్యంగా తనకు బాగా తెలిసిన స్నేహితుడిగా గాని, బంధువు గా గాని లేకపోతే తను పని చేస్తున్న ప్రదేశంలో బాగా పరిచయం ఉన్న వ్యక్తి వల్లె వాళ్ళ పేరు చెప్పి అవతలి వ్యక్తి నటిస్తాడు.

4. Whatsapp లోనే తమకు ఎమర్జెన్సీ లో ఉన్నానని, హాస్పిటల్ ఉన్నానని, లేకపోతే తనకు అర్జెంటు మనీ అవసరం వచ్చిందని ఎలాగైనా సహాయం చేయమని భాదితుని అడిగి మరుసటి రోజేమనీ తిరిగి పంపిస్తానని నమ్మిస్తాడు.
5. భాదితుడు పైన చెప్పిన విషయం నమ్మి తనకి తెలిసిన వక్తే కదా అని, అతడు ఎమర్జెన్సీలో ఉన్నందున మని అడుగుతున్నట్లు అనుకుంటాడు.
6. అంతలొ ఎవరి పేరైతే చెప్తారో వాళ్ళకి కాల్ చేద్దామని అనుకొనే లోపు అవతలి వ్యక్తి ప్రస్తుతం నా పాత నెంబర్‌కి కాల్ అవ్వటం లేదని చెప్తాడు.
7. కాబట్టి భాదితుడి ఫోన్ చేయాలనే ఆలోచన విరమించుకుంటాడు. అలాగే అతడు ఆలోచించడానికి అవకాశం లేకుండా డబ్బులు పంపమని కంగారు పెడతాడు.
8. వెంటనే భాదితుడు డబ్బులను అవతలి వ్యక్తికి పంపుతాడు.
9. తర్వాత భాదితుడు తాను డబ్బులను పంపింది తనకు తెలిసిన వారు కాదని సైబర్ నేరగాళ్ళు అని తెలిసి మోసయోయానని గ్రహిస్తాడు.



హని ట్రాప్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... హాని ట్ర్యాప్ చేస్తూ లక్షల్లో అమౌంట్ దోచుకుంటున్న సైబర్ నేరగాళ్ళు సమాజంలో హై ప్రోఫైల్ గల వ్యక్తులను సోషల్ మీడియా వెబ్‌సైట్ అయిన ఫేస్‌బుక్/ ఇన్‌స్ట్రాగ్రామ్ మొదలగు వారియొక్క వివరాలు సేకరించి వారిని టార్గెట్ ఏసి వారికి న్యూడ్ వీడియో కాల్ చేసి కవ్వించే విధంగా మాట్లాడి వారిని కూడా న్యూడా గా ఉండమని రిక్వెస్ట్ చేసి, ఆ వీడియో ని రికార్డు చేసి దాన్ని వారి యొక్క పెరెంట్స్‌కి మరియు అన్ని సోషల్ మీడియా వెబ్‌సైట్‌లలో అప్లోడ్ చేస్తామని బయపెట్టి లక్షల్లో అమౌంట్ దోచుకుంటారు.

నేర విధానం వివరంగా :

1. మొదటిగా భాదితుడికి ఒక తెలియని యంగ్ లేడీ నుండి ఫేస్‌బుక్/ ఇన్‌స్ట్రాగ్రామ్ మొదలగు నుండి ఫ్రెండ్ రిక్వెస్ట్ వస్తుంది. బాధితుడు ఆ ఫ్రెండ్ రిక్వెస్ట్ ను అక్సెప్ట్ చేస్తాడు. అంతట ఆ లేడి బాధితుని యొక్క ఫ్రెండ్స్ లిస్టు అంత కాపీ చేసుకుంటుంది.
2. అనంతరం ఆ లేడి బాధితునితో ఒంటరిగా ఉన్నట్టు మీతో స్నేహ పూర్వకముగా కవించే విధంగా ఛాటింగ్ చేసి, మీ వాట్స్‌ప్ నెంబర్ ఇవ్వమని అడిగి మిమ్మల్ని వాట్స్‌ప్‌లోకి రమ్మని చెబుతారు.
3. తరువాత బాధితున్ని వాట్స్‌ప్ లో వీడియో కాల్ చేయమంటారు. లేదా ఆ లేడి వీడియో కాల్ చేస్తుంది.
4. ఆ వీడియో కాల్‌లో ఆ లేడీ న్యూడా గా కనిపిస్తుంది మిమ్మల్ని తన హావభావాలతో రెచ్చగొట్టి మిమ్మల్ని కూడా న్యూడ్ గా కనిపించమని చెబుతుంది బాధితుడు అమె యొక్క రెచ్చగోట్టే మాటలకు మెస్మరైస్ అయ్యి ఆ లేడి చెప్పిన విధముగా న్యూడ్‌గా కనిపిస్తాడు.

5. ఆ లేడీ ఆ వీడియో కాల్‌లో బాధితుని యొక్క న్యూడ్ వీడియో రికార్డు చేస్తుంది. అనంతనరం ఆ వీడియో ని బాధితుడికి పెట్టి తాను కాల్ గర్ల్ అని చార్జస్ పే చేయాలని డబ్బులు తను చెప్పిన అకౌంటు లో వెంటనే వేయాలని ఫేస్‌బుక్ / ఇన్‌స్ట్రాగ్రామ్/ యూట్యూబ్/ పోర్న్‌సైట్ ఇతర సైట్ లలో పెడతానని బయపెడుతుంది.
6. బాధితుడు అందరికి తెలిస్తే పవువు పోతుంది తీవ్ర మనోవేదనకు లోనై ఆమె చెప్పిన అకౌంట్‌లో డబ్బులు వేస్తాడు.
7. అనంతరం ఆమె యొక్క ఏజెంట్ అని ఫోన్ చేసి అతను చెప్పిన అకౌంట్‌లో డబ్బులు వేయాలని లకుంటే ఫేస్‌బుక్ / ఇన్‌స్ట్రాగ్రామ్ మొదలగు న్యూడ్ వీడియో / ఫోటోలు అప్లోడ్ చేస్తానని చెప్పి బయపెట్టి ఒక్కో న్యూడో ఫోటో ని బాధితుని ఫ్రెండ్స్ కి పోస్ట్ చేస్తాడు. అది డిలీట్ చేయాలంటే డబ్బులు వేయమంటాడు. బాధితుడు డబ్బులు అకౌంట్‌లో వేస్తే ఒక్కో ఫోటో డిలీట్ చేస్తాడు. ఈ విధంగా ఆమె దఫదఫలుగా ఎక్కువ మొత్తములో అమౌంట్ వేయిన్చుకుంటుంది.
8. భాధితుడు డబ్బులు వేయటానికి లేట్ లేదా అమౌంట్ అకౌంట్‌లో వేయకపోయిన, ఇంకో Fraudster ఫోన్ చేసి డిల్లీ నుంచి సైబర్ క్రైమ్ / సిబిఐ ఆఫీసర్‌ని మాట్లాడున్నానని మీరు ఒక లేడీ కి న్యూడ్ కాల్ చేసి వీడియో Youtube అప్లోడ్ అయింది. Youtube లో ఎంతో మంచి చిన్నపిల్లలు, మహిళలు వీడియోస్స్ చూస్తూంటారు. ఇలాంటి న్యూడ్ వీడియోస్ యూట్యూబ్ లో పోస్ట్ చేయకూడదు అని మాకు దీనిపై దర్యాప్తు చేయమని కంప్లైంట్ వచ్చింది అని , మీ FIR ఫైల్ చేసి మ్మిల్ని అరెస్ట్ చేస్తారని అగ్రసివ్‌గా మాట్లాడతారు.
9. అంతట బాధితుడు ఆ లేడీ ఏ నూడ్ కాల్ చేసి రెచ్చగొట్టి తనని న్యూడ్ కాల్ చేయమంది అని సమాజంలో తనకంటు ఒక గుర్తింపు ఉందని, ఈ విషయం అందరికి తెలిస్తే పరువు పోతుంది అని ప్రదయపడతాడు
10. అంతగ ఆ Fake సిబిఐ / సైబర్ క్రైమ్ ఆఫిసర్ బాధితుడి యొక్క బాధని అర్ధం చేసుకున్నట్లు బాధితునుకి సహకరిస్తున్నట్లు నటించి. మీ వీడియో యూట్యూబ్ లోపోస్ట్ అయింది కావున వెంటనే యూట్యూబ్ వాళ్ళకి ఫోన్ చేసి డిలీట్ చేయించండి. అని ఒక Fake Youtube మేనేజర్ మొబైల్ నెంబర్ బాధితుడకి ఇస్తాడు.
11. భాదితుడు ఆ Fake youtube మేనేజర్‌కి ఫోన్ చేసి తన యొక్క విడియో డిలీట్ చేయమని రిక్వెస్ట్ చేస్తాడు. అంతట ఆ Fake youtube మేనేజర్ ఆ వీడియో డిలీట్ చేయాలంటే మీరు కొంత డబ్బు కట్టాలని చెబుతాడు.లేదంటే మీపై కేసు నమోదు చేయిస్తామని బయపెడతాడు.
12. బాధితుడు తప్పని సరి పరిస్థితులో ఆ Fake youtube మేనేజర్ కి డబ్బులు అకౌంట్ లో వేస్తాడు.
13. అదే మాదిరిగా ఫేస్‌బుక్ / ఇన్‌స్ట్రాగ్రామ్ లో కూడా ఆ వీడియోస్ డిలిట్ చేయడానికి బాధితుడు దానికి సంబంధించిన Fake మేనేజర్ లకి డబ్బులు వేయవలసివస్తుంది.

14. తరువాత మరి కొన్ని రోజులకి మరల ఇంకో ఫేక్ సిబిఐ / సైబర్‌క్రైమ్ / ఆధర్ పోలీస్.ఆఫిసర్ ఫోన్ చేసి న్యూడ్ వీడియో కాల్ లో మాట్లాడిన అమ్మయి మేడపై నుండి దూకి సూసైడ్ చేసుకుంది ని ఆమె ఫోన్ లో ఈ విడియో వుంది అని మీపై కేసు నమోదు చేసి అరెస్ట్ చేయాలని బయపేడతారు మీపై కేసు లేకుండా చేయాలంటే మీరు కొంత డబ్బు కట్టాలని చెబుతారు.

15. బాధితుడు తన బాధ ని ఎవరికి చెప్పుకోలేక తీవ్ర మానసిక క్షోభకు లోనై Fraudster కు ధపదఫాలుగా లక్షల్లో అమౌంట్ వారు చెప్పిన అకౌంట్స్ లో వేసి మోసపోతాడు.





బిజినెస్ ఈమెయిల్ కాంపర్మైస్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... BUSSNESS EMAIL COMPROMISE పేరుతో Fraud చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు ఈ మధ్యకాలంలో ఎక్కువగా జరుగుతున్న సైబర్ నేరాలలో ఈమెయిల్ స్నూపింగ్ అనే పద్ధతిని ఉపయోగించి ఇద్దరి ప్రముఖ వ్యక్తుల మధ్య లేదా రెండు సంస్థల మద్య లేదా రెండు బిజినెస్ లా మధ్య జరిగిన సున్నితమైన ముఖ్యమైన ఇన్ఫర్మేషన్ను వాళ్ళకు తెలియకుండా ఈ సైబర్ నేరగాళ్ళు ఈమెయిల్ స్నూపింగ్ (Email Snooping) ఉపయోగించి ఎప్పటికప్పుడు సిక్రేట్ గా అబ్జర్వ్ చేస్తూ ఉంటారు. ఇది తెలియని సందరు వ్యక్తులు లేదా కంపెనీ వాళ్ళు సున్నితమైన ఇన్ఫర్మేషన్ ని ఈమెయిల్ ద్వారా పంపించుకుంటూ ఉంటారు. అలాంటి ముఖ్యమైనన సనమాచారాన్ని దొంగలించిన సైబర్ నేరగాళ్ళు దాన్ని ఉపయోగించుకొని ఈ మెయింల& స్పోఫింగ్ (Email spoofing) పద్ధతిలో కొత్తగా వేరే ఈమెయిల్ ఐడి ని అదే పేరుతో కొత్త డమైన్తో క్రియేట్ చేస్తారు. ఆకొత్త ఈమెయిల్ ను ఉపయోగించి వారు ముందుగానే మాట్లాడుకున్న బిజినెస్ డీల్ను లేదా ఇన్ఫర్మేషన్ ను ఉపయోగించి సదరు కంపెనీ వారికీ పంపి అకౌంటు మారింది అని చెప్పి మానీ టేరాన్సాక్షన్ లేదా ఇంపార్టెంట్ విషయాన్ని పంచుకన్నప్పుడు ఆ విషయాన్ని వాళ్ళు తస్కరిస్తారు.

నేర విధానం వివరంగా :

- Email snooping:
  1. ఈమెయింల్ స్నూపింగ్లో ముఖ్యంగా ఇద్దరు వ్యక్తులు మధ్య లేదా రెండు బిజినెస్ లు మధ్య జరిగే సంభాషణఋ సిక్రేట్గా స్నూపింగ్ పద్ధతిలో సైబర్ నేరగాళ్ళు గమనిస్తూ ఉంటారు. దీనివల్ల అవతం వ్యక్తుల మధ్య జరిగే సున్నితమైన ఇన్ఫర్మేషన్ బయటకు వెళ్ళే ప్రమాదం ఉన్నది.

Email spoofing:

1. ఈ-మెయిల్ స్పూఫింగ్ ద్వారా తెలుసుకున్న ముఖ్యమైన సమాచారాన్ని లేదా సున్నితమైన సమాచారాన్ని సైబర్ నేరగాళ్ళు ఉపయోగించి ముందు కనిపించే ఈమెయిల్ లానే అదే విధంగాడోమైన్ మార్చి కొత్త ఈమెయిలన్ క్రియేట్ చేస్తారు.
2. ఆ కొత్తగా తయారు చేసిన ఈమెయిల్‌తో ఏ కంపెనీ నుంచి అయితే ఇన్ఫర్మేషన్‌ని దొంగలించాలని అనుకుంటున్నారో వాళ్ళకు తమ పాత క్లైంట్ లాగే వ్యవహరిస్తూ మెయిల్ చేస్తారు.
3. ఆ మెయిల్ రిజీవ్ చేసుకన్న సదర్ కంపెనీ వారు పైన కనిపించే పేరును మాత్రమే చూసి డొమైన్ చూడకుండా ఎప్పటిలానే వారు తమ యొక్క బిజినెస్ డీల్‌నీ లేదా ఇంపార్టెంట్ విషయాన్ని ఆ మెయిల్ చర్చుస్తారు.
4. ఈ ముఖ్యమైన ఇన్ఫర్మేషన్ లో మనీ టర్న్ క్షన్ కి సంబంధించినది అయితే సైబర్ నేరగారు తమయొక్క బ్యాంక్ ఆకౌంట్ లను పెట్టి కంపెనీకి పంపిస్తాడు.
5. ఈ విషయం తెలియని సదరు కంపెనీ వారు ఆ అకౌంట్ కి తాము కుదుర్చుకున్న పాత డీల్ ప్రకారం డబ్బులను కొన్ని లక్షలో పంపించి మోసపోతాడు.
6. ఒకవేళ సదర్ కంపెనీ వారు ఆ మెయిల్‌లో ఏదైన ఇంపార్టెంట్ సమాచారాన్ని పంపిస్తే ఆ సమాచారాన్ని ఉపయోగించి మీరు మేము అడిగినంత డబ్బులు పంపించకపోతే దీన్ని దుర్వినియోగం చేస్తామని బెదిరిస్తారు.
7. చేసేదేమి లేక సదరు కంపెనీ వారు వాళ్ళకి అడిగినంత డబ్బులను పంపి చివరకు సైబర్ నేరగాళ్ళ చేతుల్లో మోసపోతున్నారు.



విషింగ్ ఫ్రాడ్ ఫేక్ కాల్స్ ఇన్ ద నేమ్ ఆఫ్ సిఐయస్ఎఫ్ (ఆర్మీ) ఫర్ మెడికల్ టెస్ట్స్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... CISF (Army) పేరుతో Fraud చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు..., ఫేక్ ఫోన్ నంబర్స్ తో మనకి (ఎవరితే మెడికల్ ల్యాబ్స్) నడుపుతారో వారకీ ఫోన్ చేసి మేము Central Reserved Force అయోనట్టు వంటి CISF, CRPF లో పనిచేస్తునము అని చెపుతారు. మా స్టాఫ్‌కి 20 నుండి 30 మందికి మెడికల్ టెస్ట్స్ చేయాలి అని చెప్పుతారు. తరువాత వారి Army Process ప్రకారం మీరు Whats app వీడియో కాల్ చేసి Phonepe ఓపెన్ చెయాలి అంటారు అడ్వాన్సు పంపిస్తాము దాని కోసం మీరు ఫోన్ పే లో మీ క్రెడిట్ అండ్ డిబిట్ కార్డ్స్ అన్ని Add చేయాలి తరువాత మీ దగ్గర నుంచి మేము ఇచ్చిన UPIID కి అడ్వాన్సు పే చేస్తే రేటింపు అయి వస్తుంది అంటారు కానీ రాదు ఆలానే ఇంకో వధంగా మా అకౌంట్స్ మీ UPI లో Add చేసుకొని మేము చెప్పిన విధంగా చేస్తే మీకు మేము పంపిన అడ్వాన్సు వస్తుంది అని చెప్పి మన దగ్గర నెంచే డుబ్బలు వేయింరుకొని మోసం చేస్తున్నారు.

నేర విధానం వివరంగా :

-
    1. మొదటిగా భాదితుడికి (ఎవర్రైతే మెడికల్ Labs నడుపుతారో) వారికి ఒక తెలియని ఫక్షన్ నెంబర్ నుంచి ఫోన్ వస్తుంది అది లిఫ్ట్ చేసిన తరువాత, మేము Central Reserved Force ఆయోనట్లు వంటి CISF, CRPF పనిచేస్తునాను. మా స్టాఫ్ కి 20 నుంచి 30 మందికి మెడికల్ టెస్ట్స్ చేయాలి అని చెప్పుతారు.

2. భాదితుడు అది నిజం అని నమ్మిన తరువాత అడ్వాన్సు ఎంత ఇవ్వాలి అని మాట్లాడుతారు.
3. ఒక రేట్ ఫిక్స్ అయి తరువాత మా Central Reserved Force అయోనట్టు వంటి CISF, CRPF లో ఒక Process ఉంది దాని ప్రకారం చేయాలి అని అంటాడు.
4. అందులో మొదటిగా మీరు Whatsapp వీడియో కాల్ చేసి ఫోన్ పే ఓపెన్ చేయాలి అంటారు. అడ్వాను& పంపిస్తాము దాని కోసం మీరు ఫోన్‌పే లో మీ క్రిడెట్ అండ్ డెబిట్ కార్డ్స్ అన్ని Add చేయాలి అని అంటారు.
5. తరువాత మీ దగ్గర నుంచి మేము ఇచ్చిన UPI ID కి పే చేస్తే రెట్టింపు అయి వస్తుంది అంటారు కీనీ రాదు, మన అకౌంట్ నుంచి డబ్బులు డెబిట్ అవుతాయి, ఏంటని వాడిని అడుగగా వాడు సార్ మీకు వస్తుంది ఎదో ఎర్రర్ చూపిసుతష్త్ర&ందని అంటారు అని నిజమని మళ్ళా డబ్బులు వేస్తాం కానీ రిటర్న్ రాదు.
6. మళ్ళీ ఫోన్ చేసేసరికి వాళ్ళు సిస్టం లో ఏదో ప్రోబ్లమ్ ఉంది ఎర్రర్ వస్తుంది ఇంకోసారి ప్రయత్నించండి ఇంకొకసారి కూడా వేస్తా కానీ ఎన్నిసార్లు చేసినా సరే మన డుబ్బులు పోవడం తప్ప మనకి తిరిగి రావు అప్పుడు బాధితులు ఇది మోసం అని అర్ధం చేసుకుంటారు.
7. రెండో విధంగా మీకు మేము పంపిన అడ్డాన్సు రావాలి అంటే మీరు మేము పంపిన అకౌంటు ని మీ UPI Payments లో Add చేసుకోండి అనిచెపుతారు.
8. అది నిజం అని నమ్మి మన UPI అకౌంట్ Add చేసుకున్న తరువాత మనం ఎంత అడ్వాన్సు అనుకునమో అ అమౌంట్ టైపు చేసి Recipient దగ్గర మన పేరు Add చేయమాన్ని చెపుతాడు.
9. అలా చేసిన తరువాత భాదితుడు UPI PIN ఎంటర్ చేయవలసి ఉంటుంది. పిన్ ఎంటర్ చేసిన వెంటనే మన అకౌంట్ లోనుంచి డబ్బులు డెబిట్ అవుతాయి.
10. భాదితుడు వెంటనే Fraudster కి అడిగితే లేదు మీ డబ్బులు మీకు refund అవుతాయి మొత్తం అడ్వాన్సుతో కలిపి ఇంకో సరి అలానే చేయండి అని అంటాడు.
11. భాదితుడు అది నిజం అని నమ్మి అలా చేసిన వెంటనే మరోసరి డబ్బులు కట్ అవుతాయి.
12. ఈ విధంగా బాధితుడు సైబర్ మోసగాళ్ళు చేతిలో డబ్బులు వేసి మోసపోతారు.

ఫేక్ ట్రాయ్ కాల్ ఫ్రాడ్

(టెలిగ్రామ్ రెగ్యులేటరి ఆథరైజడ్ ఆఫ్ ఇండియ)



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... TRAI (Telecom Regulatory Authority of Indai) పేరుతో Fraud చేస్తున్న సైబర్ నేరగాళ్ళు ఫేక్ ఫోన్ చేసి Trai నుంచి ఫోన్ చేస్తున్నాము మీ పేరు, ఆధార్ మీద ఫోన్ నెంబర్ రిజిస్టర్ అమి ఉంది అది ముంబైలో ఉన్న వ్యక్తి వాడుతున్నారు దానితో వివిద రకాల ఈలిగల్ యక్టివిటీస్ మరియు ఈల్లిగల్ మేసెజస్ జరుగుతు ఉన్నాయి అని చెప్పి మనలని భయభ్రంతులకు గురిచేసి వారు చెప్పిన అక్కౌంట్స్ లో డబ్బులు వేయించుకొని మోసం చేస్తున్నారు.

నేర విధానం వివరంగా :

-

1. మొదటిగా భాదితుడికి ఒక తెలియనని ఫోన్ నెంబంర్ నుంచి ఫోన్ వస్తుంది అది లిఫ్ట్ చేసిన తరువాత మేము TRAI (Telecome Regulatory Authority of India నుంచి ఫక్షన్ చేస్తున్నాము అని చెప్పి మీ పేరు, ఆధార్ మీద ఫోన్ నెంబర్ రిజిస్టర్ అయి ఉంది అది ముంబైలో ఉన్న వ్యక్తి వాడుతున్నారు దానితో వివిద రకాల ఈలిగల్ యక్టివిటీస్ మరియు ఈల్లిగల్ మేసెజస్ జరుగుతు ఉన్నాయి అని చెబుతారు
2. భాదితుడు నేను ఏమి ఫోన్ నెంబర్ తీసుకులేదు అని చెప్పగా,అ Fraudster మీ పేరు ఆధార్ కార్డు నెంబర్ చెబుతాడు. ఆ వివరాలు అన్ని కరెక్ట్‌గా ఉండడంతో భాదితుడు కొంచం భయానికి గురి అవుతాడు.
3. సైబర్ నేరగాళ్ళు Open Source Intelligence పరికరములతో తో భాదితుడు యొక్క వివరాలు కలెక్ట్ చేయడం జరుగుతుంది ఆ వివరాలు భాదితుడుకి చెపుతారు.

4. తరువాత ముంబాయి క్రైమ్ బ్రాంచ్ వారికి లైన్ కలుపుతున్నాము. మీరు వారితో మాట్లాడండి అని చెప్పి వేరే వాళ్ళకు లైన్ కలుపుతారు అందులో walkie talkie sounds వినిపిస్తారు.
5. అంతట మరో Fraudster కాల్ లిఫ్ట్ చేసి ముంబాయి క్రైమ్ బ్రాంచి నుండి మాట్లాడుతున్నట్లు చెబుతాడు. భాదితుడు పేరు వివరాలు చెప్పగా ఆ Fraudster మీ పేరు మీద వచ్చిన పార్సెల్ గురించి అందులో గల illegal transporting items గురించి చెప్పి, దిని మీద FIR రిజిస్టర్ చేయాల్సి ఉంది అని చెప్పి, ఇతర వివరాల కోసం ఇన్స్‌పేక్టర్ గారితో మాట్లాడమని ఫోన్ వేరేవాళ్ళకి ఇస్తారు.
6. తరువాత ఇంకో Fraudster పోలీస్ ఇన్సెపెక్టర్ మాట్లాడుతున్నట్టు బాధితుడుతో మాట్లాడుతాడు. భాదితుడు ఎటువంటి పార్సెల్ పంపలేదని. తనకి illegal items గురించి ఎటువంటి అవగాహనా లేదని నిరపరాధివి అని చెప్పిన. ఆ Fraudster వినకుండా మీరు వెంటనే ముంబాయి క్రైమ్ పోలీస్ స్టేషన్ కు రావాలని చెబుతారు. బాధితుడు వేరే లోకేషన్‌లో ఉన్నాను అని చెప్పగా Whatsapp/Skype ద్వారా మిమ్మల్ని కనెక్ట్ చేస్తాము. మేము అడిగిన ప్రస్నలన్నింటికి కరెక్ట్‌గా సమాధానం చెప్పాలని మీరు ఒంటరిగా ఉండాలి ఎవరు మీ దగ్గరలో ఉండకుడదు అని ఇన్వెస్టిగేషన్ కు సపోర్టు చేయాలని లేదంటే మీరు, మీ ఫ్యామిలీ అంతటిని అరెస్ట్ చేయాల్సి ఉంటుందని బయపెడతారు.
7. బాధితుడుకి Whatsapp / skype ద్వారా వీడియో కాల్ చేస్తారు. అక్కడ పోలీస్ యూనిఫారంలో ఇన్సెక్టర్ రెస్‌లో Fraudster కనిపిస్తాడు.
8. బాధితునికి వివిధరకాల ప్రశ్నలు వేసి, బాధితుని యొక్క పూర్తి వివరాలు అతని బ్యాంకు ఖాతా మరియు బ్యాలెన్స్ వివరాలు తెలుసుకుంటారు. ఇంతలో సిబిఐ నుండి ఇన్వెస్టిగేషన్ అంత Confidential ఉంచడానికి అంగికరిస్తునట్లు అగ్రిమెంట్ వచ్చింది అని CBI పేరుతో ఒక అగ్రిమెంట్ కాపి బాధితునికి పంపుతారు. అది చూసి బాధితుడు ఇంకా బయపడతాడు.
9. తరువాత బాధితుడుతో ఇంకా FIR ఫైల్ చేయలేదని, మీరు ఎటువంటి పార్సెల్ పంపలేదు అంటున్నారు కావున మా ACP గారితో మాట్లాడండి అని ఫోన్‌కాల్ వేరే వాళ్ళకి ఇస్తాడు. అతను చాల సిరియస్‌గా మాట్లాడి వెంటనే FIR చేసి తనదగ్గర పెట్టమని చెబుతారు ఇన్స్పెక్టర్‌గా మాట్లాడిన వ్యక్తి ఇన్వెస్టిగేషన్‌కు సహకరిస్తున్నాడని బాధితునికి సపోర్ట్ చేసిన విధంగా మాట్లాడుతాడు.
10. అప్పుడు ఆ ACP సరిగా వెరిఫై చేయమని సూచనలు ఇస్తాడు.
11. అనంతరం ఒక Fake SUPREME COURT ORDER పంపుతారు.
12. భాదితుడు అది నిజం అని నమ్మి తన దగ్గర ఉన్న డబ్బులు అన్ని వాళ్ళ చెప్పిప అకౌంట్‌కి బదిలి చేస్తాడు. ఈ విధంగా భాదితుడు సైబర్ మోసగాళ్ళ చేతిలో డబ్బులు వేసి మోసపోతారు.

హ్యాకింగ్ ఫోన్ త్రూ టెలిగ్రామ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... Telegram Application ద్వారా మన మోబైల్ ఫోన్ ను హ్యాకింగ్ చేస్తూ చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు టెలిగ్రామ్ అప్లికేషన్ లో మనకు తెలియని చాలా ఛానల్స్ నుంచి మనం ఉచితంగా రీసెంట్ సినిమాలు, వెబ్ సిరీస్లు డౌన్లోడ్ చేసుకోవటం జరుగుతుంది కాని ఇలా డౌన్‌లోడ్ చేయటం వలన మనకు తెలియకుండా ఆ ఫైల్ తో పాటు బ్యాక్‌గ్రౌండ్ లో Spyware, Terra Spyware మన ఫోన్ లోకి ఎటాక్ అయ్యి ఒక spy లా నిరంతరం మన ఫోన్‌లో చేసే యాక్టివిటీస్ ను హ్యాకర్ కు చేరవేస్తుంది. అలాగే మన ఫోన్ ను మన కంట్రోల్ లేకుండా చేస్తుంది. మరియు మన Identy మీద మనకు తెలయకుండా లోన్స్ తీసుకోవటం జరుగుతుంది.

నేర విధానం వివరంగా :

-

1. ఈ రోజుల్లో చాలా మంది చాలా అవసరాల కోసం టెలిగ్రామ్ అప్లికేషను ను ఉపయోగించటం జరుగుతుంది. దాని ద్వారా ఎక్కువ GB కలిగిన ఫైల్స్ సులువుగా టన్స్ఫర్ చేసుకోవచ్చు.
2. ప్రస్తుతం చాలా మంచి OTT ను Subscribe చేసుకోకుండా Free గా HD Quality కలిగిన సినిమాలు మరియు వెబ్ సిరీస్ ను డౌన్లోడ్ చేసుకోవటం జరుగుతుంది.

3. ఇదే అవకాశం గా భావించి సైబర్ మోసగాళ్ళు ఫేక్ టెలిగ్రామ్ చానల్ ను టెలిగ్రామ్ లో Run చేస్తూ కొత్త సినిమాలు మరియు వెబ్‌సిరీస్ ను ఆ ఛానల్ లో Upload చేస్తూ వాటితో పాటు భాదితునికి తెలియకుండా spyware ని ఆ ఫైల్ కి అటాచ్ చేస్తున్నారు.
4. ఇది తెలియని భాదితుడు ఆ సినిమాలు డౌన్లోడ్ చేసే క్రమంలో spyware కూడా ఆ ఫైల్స్ తో కలిపి తన ఫోన్‌లోకి డౌన్లోడ& చేసుకుంటున్నాడు.
5. ఆ spyware ఒక మొబైల్ spy లాంటిది. అది ఆ సినిమాను డైన్లోడ్ చేసుకున్న వారి ఫోన్ లో చేసే ప్రతి విషయం అనగా కాల్ రికార్డింగ్స్ ఫోన్ లోకేషన్స్ ఫోటోస్ రియల్ టైం లోకేషన్ Browsing Activitis, CAMERA Access ఫోన్‌లో ఉండే ముఖ్యమైన Password లాంటి సమాచారాన్ని Hacker కు చేరవేస్తుంది.
6. ఇటువంటి సమాచారాన్ని మనకు తెలియకుండా దొంగలించటం వలన మన Identity మీద లోన్స్ తీసుకోవటం అమ్మాయిల ఫోటోస్‌ను మార్ఫ్ చేయడం మన లానే మన కాంటాక్ట్స్ తో ఛాటింగ్ చేయటం ప్రవేట్ సమాచారాన్ని దొంగాలించటం జరుగుతుంది.

సైబర్ క్రైమ్ అవేర్నెస్ :

యావన్మంది ప్రజానీకానికి సైబర్ క్రైమ్ పోలీసు వారి విజ్ఞప్తి తెలియని టెలిగ్రామ్ ఛానల్స్ లో సినిమాలు మరియు వెబ్ సిరీస్ డౌన్‌లోడు చేయవద్దు. దాని ద్వారా spyware ఎటాక్ అయి ఫోన్ లో చేసే ప్రతి activity అనగా కాల్ రికార్డింగ్స్ ఫోన్ లోకేషన్స్ ఫోటోస్, రియల్ టైం లోకేషన్ rowing activities Camers Access ఫోన్ లో ఉండే ముఖ్యమైన పాస్వర్డ్స్ లాంటి సమాచారాన్ని హ్యాకర్ చేరవేస్తుంది.

ఇండియాన్ ఈ- కామర్స్ ఫ్రాడ్

సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... ఇండియాన్ మార్ట్ వెబ్‌సైట్ లో కస్టమర్ సెర్చ్ చేసినట్లు వంటి సమాచారం ఆధారంగా సైబర్ నెరగాళ్ళు వారికి ఫోన్ చేసి వారికి కావలసిన ప్రోడక్ట్సని తక్కువ ధరకే ఇస్తాం అని చెప్పి నమ్మించి ఎక్కువ మొత్తంలో డబ్బులు వారి ఎకౌంట్‌లో వియించుకుంటూ అమాయక ప్రజలని మోసగించి దోచుకుంటున్న సైబర్ నేరగాళ్ళు.

నేర విధానం వివరంగా :

•

1. ఏమైనా వస్తువుల్ని గాని, మిషనరీ గాని వాటి యొక్క ఉత్పత్తి దారులు లేదా సప్లయర్స్ వద్ద తక్కువ ధరకే కొనడానికి వ్యాపారస్తులు, ఎంటర్రైఐన్యూర్ మరియు సామాన్య ప్రజల ఇండియా మార్ట్ అనే వెబ్ సైట్లో లాగిన్ అయ్యి ఆ ప్రోడక్ట్స్ పేరుతో సెర్చ్ చేస్తారు.
2. అంతట సదరు కొనుగోలు దారుడుకి ఆయా ప్రొడక్ట్స్ సప్లయర్ లిస్టు వారి యొక్క వివరాలు కనిపిస్తాయి మరియు ఆ వస్తువుల అమ్మే సప్లయర్స్ కి ఆ వస్తువులు కోసం ఎవరు సెర్చ్ చేస్తారో వారి పేరు, ఫోన్ నెంబంర్ కనిపిస్తాయి.
3. సైబర్ నేరగాళ్లు కూడా ఇదే ఇండియన్ మార్ట్ వెబ్ సైట్ లో కొనుగోలు దారుడు సెర్చ్ చేసినటువంటి డేటా ఆధారంగా ఆ వ్యక్తి యొక్క పేరు ఫోన్ నెంబర్ తెలుసుకొని ఆఫోన్ నెంబర్‌కి కాల్ చేసి ఇండియన్ మార్ట్‌లో వాళ్ళు సెర్చ్ చేసినటువంటి వస్తువులు సప్లై చేస్తాం అని చెబుతారు.
4. కొనుగోలు దారుడుకి ఏమి కావాలో అవి తక్కువ ధరలోనే ఇస్తామని నమ్మించి బేరం కుదుర్చుకుంటారు.
5. కొనుగోలుదారుడుని నమ్మించడానికి వారి వద్ద గల ఆ ప్రోడక్ట్స్ ఫోటోస్ ఒక ఫేక్ జీఎస్టీని, ఇడెంటీ కార్డు ఇతర ప్రూఫ్స్ ని వాట్సాప్ ద్వారా పంపుతాడు.
6. ఫ్రాడ్‌స్టర్ తన యొక్క బ్యాంకు అకౌంట్ నెంబర్ ను కొనుగోలు దారునుకి ఇచ్చి ముందుగా 50% అమౌంట్ డిపాజిట్ చేయమంటాడు మరియు ఒక తప్పుడు ఇన్వాయిస్ కూడా పంపిస్తాడు.
7. అనంతనం ఫ్రాడ్‌స్టర్ లారి డ్రైవర్ లా ఫోన్ చేసి లారి మధ్యలో ప్రాబ్లమ్ వచ్చింది వెంటనే కొండ డబ్బు వేయండి ఒక రోజులో మేము అక్కడికి వచ్చి మీ డబ్బులు ఇచ్చేస్తాను అని చెబుతారు.
8. ఈ విధంగా చాలా రకాలుగా చెపిప్ప బాధితుడు దగ్గర నుంచి డబ్బులు వేయించుకుంటారు.

వాట్సప్ హ్యాకింగ్



సిటీ నగర ప్రజలకు సైబర్ క్రైమ్ పోలీసు వారి సమాచారం. తస్మాత్ జాగ్రత్త... WHATSAPP ను HACKING చెస్తు చెలరేగిపోతున్న సైబర్ నేరగాళ్ళు వాట్సప్ అప్లికేసను కు ఒక ఫేక్ నెంబర్ తో మనకు తెలిసని వాళ్ళ యొక్క వాట్సప్ ని హ్యాక్ చేసి భాదితుడి యొక్క వాట్సప్ లో అతని యొక్క కాంటాక్ట్స్ మరియు whatsapp groups లో malware కలిగిన ఒక APK ఫైల్ ని పంపించడం జరుగుతుంది. ఆ APK ఫైల్ పంపించడం జరుగుతుంది. ఆ APK ఫైల్ ని ఎవరైతే తెలియక క్లిక్ చేస్తారో వాళ్ళ యొక్క వాట్స్‌ప్ హ్యాక్ అవుతుంది. దాంతో వారికి తెలియకుండానే వాళ్ళ వాట్స్‌ప్ నుండి వాళ్ళ కాంటాక్ట్ అందరికి మాల్‌వార్ తో ఉన్న APK ఫైల్ Forward అవుతుంది. ఈ విధంగా భాదితేడే తపరి తెలియని మాల్‌వార్ APK ఫైల్ ను ఓపెన్ చేయడం వాళ్ళ తన యొక్క ఐడెంటిటీ ని సైబర్ నేరగాళ్ళు కాజెస్తున్నారు.

నేర విధానం వివరంగా : •

1. మొదటిగా భాదితుడికి ఒక తెలియని వాట్స్‌ప్ నెంబర్ ద్వార ఒక APK ఫైల్ ముఖ్యమైన ఇన్ఫర్మేషన్‌తో ఉన్నట్లు మనకి ఆ మెసేజ్‌లో కనిపిస్తుంది. (ఉదా: Government Jobs 2024 ApplyNow. apk)
2. భాదితుడికి అది నిజమని నమ్మి దాంతో ముఖ్యమైన ఇన్ఫర్మేషన్ పొందవచ్చునని ఆ APK ఫైల్ ను ఓపెన్ చేస్తాడు.
3. ఆ APK ఫైల్ ఓపెన్ చేసిన వెంటనే మనకి తెలియకుండానే మన ఫోన్‌లో malware Attack అయ్యి మన ఫోన్ కి వచ్చే text మెసేజెస్‌లను సైబర్ నేరగాళ్ళకు చేరవేయడం జరుగుతుంది.

4. దీని ద్వార మన యొక్క ఫోన్ నెంబర్ తో ఉన్న వాట్సప్ వేరే డివైస్ లో ఇన్‌స్టాల్ చేసినపుడు మన ఫోన్ కి వచ్చే OTP ని సైబర్ నేరగాళ్ళు వెళ్ళడం.

5. ఇదే విధంగా UPI Apps అయిన Phonepe, Google pay, Paytm etc మొదలగు వాటిని కూడా ఎలడరా చేయడానికి ప్రయత్నం జరుగుతుంది.

6. అలాగే భాదితుడి లానే అతని వాట్సప్ లో అతని కాంటాక్ట్ కి మరియు అతని వాట్సప్ గ్రూప్ కి ఇదే malware తో కూడిన apk ఫైల్ ను forward చేయడం జరుగుతుంది.

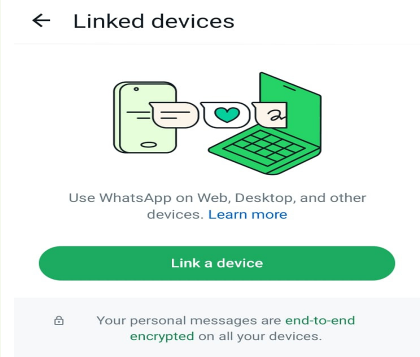
7. అయితే మిగతా వారు ఆ apk ఫైల్‌తో ఉన్న మెసేజ్ తనకు తెలిసని కాంటాక్ట్ నుంచే రావటం వాళ్ళ ఆ Apk ఫైల్ ఓపెన్ చేస్తారు. ఇలా వాళ్ళ Whatsapp ను కూడా సైబర్ నేరగాళ్ళు Hack చేస్తారు.

8. అయితే తన యొక్క whatsapp Hack అయ్యిందని, అతని యొక్క కాంటాక్ట్ నుంచి తెలుసుకున్న తరావ్వ తన వాట్సప్ ను తిరిగి లాగిన్ అవ్వటానికి ప్రయత్నించగా దానికి whatsapp లో Two - Factor Authentication PIN పెట్టినట్లు కనిపిస్తుంది, దీనితో అతడు ఆ PIN తెలియకపోవడం వల్ల తన whatsapp login ని అవ్వలేదు.

9. కానీ అతని యొక్క whatsapp నుంచి మాత్రం ఈ malware apk ఫైల్ అందరికి వెళుతూ మిగిలిన వారు కూడా పై విధంగా మోసపోవటం జరుగుతుంది.

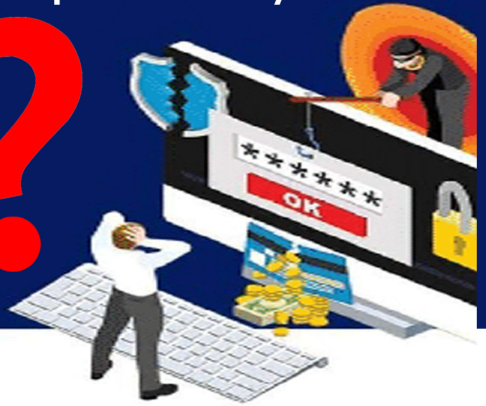
సైబర్ క్రైమ్ అవేర్నెస్ :

యావన్మంది ప్రజానీకానికి సైబర్ క్రైమ్ పోలీసు వారి విజ్ఞప్తి తెలియని నెంబర్స్ నుంచి వాట్సప్ లో మీకు ఎటువంటి malware apk ఫైల్ మెసేజ్ లు వచ్చిన వాటిని ఓపెన్ చేయవద్దు వెంటనే అటువంటి వాటిని whatsapp లో రిపోర్ట్ చేయండి.



Cyber Crime Visakhapatnam City

Are You a victim of online Financial Fraud ?





Dr. A. Ravi Shankar, IPS
Commissioner of Police &
Addl. District Magistrate
Visakhapatnam Metropolitan City
Andhra Pradesh

Immediately Call Helpline Number 1930

and register your complaint at
www.cybercrime.gov.in

Social Media Channels Visakhapatnam City Police



- https://www.youtube.com/@vizagcitypolice/
- https://www.facebook.com/visakhapatnamcitypolice/
- https://twitter.com/vizagcitypolice
- https://www.instagram.com/vizagcitypolice/
- https://whatsapp.com/channel/0029vaOHOjjHQbSDllrlat1p

web://https://sancharsaathi.gov.in